(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平9－215057

(43)公開日　平成９年(1997)８月15日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｑ	7/38			Ｈ０４Ｂ	7/26	１０９Ｒ
Ｇ０６Ｆ	1/00	３７０		Ｇ０６Ｆ	1/00	３７０Ｅ
Ｇ０９Ｃ	1/00	６６０	7259－5Ｊ	Ｇ０９Ｃ	1/00	６６０Ｄ
Ｈ０４Ｌ	9/32			Ｈ０４Ｍ	3/42	Ｚ
Ｈ０４Ｍ	3/42				11/00	３０２

審査請求　未請求　請求項の数28　ＯＬ　（全 23 頁）　最終頁に続く

(21)出願番号　特願平8－16402

(22)出願日　平成８年(1996)２月１日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　山口　宗明
東京都国分寺市東恋ケ窪１丁目280番地
株式会社日立製作所中央研究所内

(74)代理人　弁理士　小川　勝男

(54)【発明の名称】　携帯端末および携帯端末情報保護方法

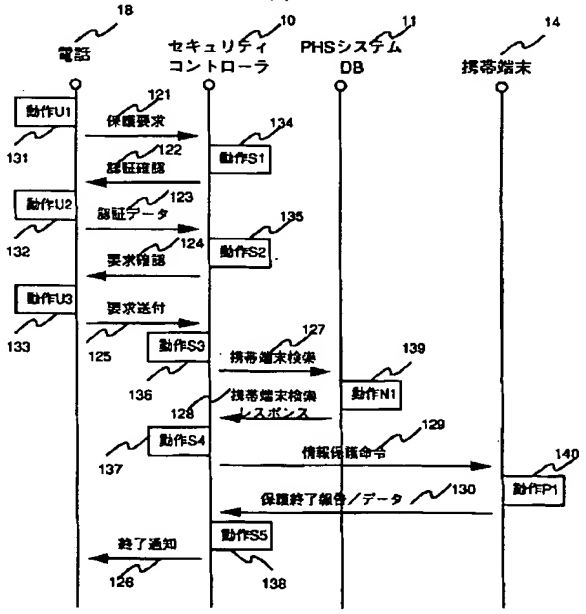
(57)【要約】

【課題】通常時の端末使用を容易にし、端末紛失時に端末内に残された個人情報の保護、回収を可能にした情報保護システムおよび携帯端末の提供。

【解決手段】携帯端末１４から発行した情報保護のための登録要求に従って、無線ネットワークに接続されたセキュリティコントローラ１０に、上記端末のセキュリティ管理データを登録しておく。端末紛失時に、携帯端末の所有者がセキュリティコントローラに情報保護を要求すると、無線ネットワークを通じて、当該携帯端末に情報保護命令が送信され、携帯端末内にある専用プログラムによって、端末内重要情報のセキュリティコントローラへの回収と無効化が行われる。

【効果】携帯端末が紛失しても重要情報を回収し、悪用を阻止できる。

図6



1

【特許請求の範囲】

【請求項１】無線通信手段と、出力手段と、入力手段と、ユーザデータを蓄積するためのメモリ手段と、上記入力手段からのユーザ操作入力に応じて、上記メモリ手段へのユーザデータの書込み、読み出し、上記出力手段への情報出力、および上記無線通信手段を介して他装置との情報の交信を行うためのデータ処理手段とからなる携帯端末装置において、

上記メモリ手段に記憶されているデータについての情報保護要求者を認証するための認証情報を記憶する手段と、

上記無線通信手段によって受信された情報保護命令メッセージに含まれる認証情報と上記記憶手段に予め記憶してある認証情報との対応関係から情報保護要求の正当性をチェックし、正当性が確認された場合に、上記メモリ手段に蓄積されている特定のユーザデータを無効化するための所定のデータ処理手順を記述した情報保護用ソフトウエアとを備え、

上記データ処理手段が、上記無線通信手段からの通知に応答して上記情報保護用ソフトウエアを実行し、上記特定のユーザデータを無効化して他人による利用を阻止するようにしたことを特徴とする携帯端末装置。

【請求項２】前記メモリ手段が、一般情報領域と保護情報領域とからなり、

前記データ処理手段が、上記情報保護用ソフトウエアを実行することにより、上記保護情報領域に蓄積されているユーザデータを無効化することを特徴とする請求項１に記載の携帯端末装置。

【請求項３】前記情報保護用ソフトウエアが、前記メモリ手段内に蓄積されている保護対象とすべきユーザデータのファイル識別情報を予め保持しており、

前記データ処理手段が、上記情報保護用ソフトウエアを実行することにより、上記ファイル識別情報で特定されたユーザデータを無効化することを特徴とする請求項１に記載の携帯端末装置。

【請求項４】前記情報保護用ソフトウエアが、ユーザデータ無効化に先立って、該当ユーザデータを前記情報保護命令メッセージの送信元に送信するための手順を含み、

前記データ処理手段が、上記情報保護用ソフトウエアを実行することにより、特定のユーザデータを他装置に回収した後、無効化することを特徴とする請求項１～請求項３の何れかに記載の携帯端末装置。

【請求項５】前記情報保護用ソフトウエアが、前記情報保護命令メッセージに含まれる処理区分コードに応じて、ユーザデータを無効化する前に、該ユーザデータを上記情報保護命令メッセージの送信元装置に選択的に送信するための手順を含み、

前記データ処理手段が、上記情報保護用ソフトウエアを実行することにより、上記ユーザデータを他装置に選択的に回収動作した後、無効化することを特徴とする請求項１～請求項３の何れかに記載の携帯端末装置。

2

【請求項６】前記情報保護用ソフトウエアが、データ消去によって前記ユーザデータを無効化させることを特徴とする請求項４または請求項５に記載の携帯端末装置。

【請求項７】前記情報保護用ソフトウエアが、データ変換によって前記ユーザデータを無効化させることを特徴とする請求項４または請求項５に記載の携帯端末装置。

【請求項８】前記情報保護要求メッセージの受信時に前記無線通信手段から出力される割込み信号に応答して、前記データ処理手段および前記メモリ手段の電源を自動的に投入動作する電源制御手段を備えたことを特徴とする請求項１～請求項７の何れかに記載の携帯端末装置。

【請求項９】携帯端末が保持しているユーザ情報の保護に必要なセキュリティ管理データをセキュリティ制御装置に登録するステップと、

携帯端末の所有者が、上記セキュリティ制御装置に対して、紛失状態にある携帯端末について情報保護を要求するステップと、

上記情報保護要求を受けたセキュリティ制御装置が、予め登録してあるセキュリティ管理データに基づいて情報保護命令メッセージを生成し、無線ネットワークを介して上記紛失状態にある携帯端末宛に送信するステップと、

上記情報保護メッセージを受信した携帯端末が、該端末内に保持する所定のユーザ情報について、他人による利用を阻止するためのデータ処理を施すステップとからなることを特徴とする携帯端末情報保護方法。

【請求項１０】前記セキュリティ制御装置が、上記情報保護を要求された携帯端末について無線ネットワークによる通信が可能な状態にあるか否かをチェックし、通信可能な状態にあることを確認して、前記情報保護命令メッセージを送信することを特徴とする請求項９に記載の携帯端末情報保護方法。

【請求項１１】前記セキュリティ制御装置が、上記情報保護を要求された携帯端末について無線ネットワークによる通信が可能な状態にあるか否かをチェックし、通信不能な状態にあった場合、上記携帯端末との無線通信可否を所定の繰返しパターンで繰り返すことを特徴とする請求項１０に記載の携帯端末情報保護方法。

【請求項１２】前記セキュリティ制御装置が、無線ネットワークに接続された移動端末データ管理装置に対して、前記情報保護を要求された携帯端末の状態を問合せ、

上記問合せを受けた移動端末データ管理装置が、上記携帯端末の位置登録の有無を上記セキュリティ制御装置に通知し、もし、現在位置が未登録状態にあった場合には、上記携帯端末について状態問合せを受けたことを記憶しておき、該当携帯端末が位置登録された時点で上記セキュリティ制御装置に通知し、

上記セキュリティ管理装置が、上記移動端末データ管理装置からの通知に応じて、前記情報保護命令メッセージを送信するようにしたことを特徴とする請求項９に記載の携帯端末情報保護方法。

【請求項１３】前記セキュリティ制御装置に登録されるセキュリティ管理データが、携帯端末のアドレス情報と、登録者識別情報と、登録者認証情報とを含み、
前記情報保護の要求時に、要求者が自分の識別情報と認証情報を提示し、上記セキュリティ制御装置が、上記提示された情報とセキュリティ管理データとして既に登録済の情報とに基づいて上記要求者の正当性をチェックし、正当性が確認された場合に、前記情報保護命令メッセージの生成と送信を行うことを特徴とする請求項９～請求項１２の何れかに記載の携帯端末情報保護方法。

【請求項１４】前記セキュリティ制御装置から送信される情報保護命令メッセージが前記認証情報を含み、
上記情報保護命令メッセージを受信した携帯端末が、該受信メッセージから抽出した認証情報と該携帯端末内に予め設定されている認証情報とに基づいて、上記受信メッセージの正当性をチェックし、正当性が確認された場合に、前記所定のユーザ情報について他人の利用を阻止するためのデータ処理を実行することを特徴とする請求項１３に記載の携帯端末情報保護方法。

【請求項１５】前記情報保護命令メッセージを受信した携帯端末が、予め指定してある所定のメモリ領域のユーザ情報について、他人の利用を阻止するためのデータ処理を施すことを特徴とする請求項９～請求項１４の何れかに記載の携帯端末情報保護方法。

【請求項１６】前記セキュリティ制御装置に登録されるセキュリティ管理データが、保護対象となる情報を特定するためのファイル識別情報を含み、前記セキュリティ制御装置が、前記情報保護命令メッセージ中に上記ファイル識別情報を設定し、
上記情報保護メッセージを受信した携帯端末が、受信メッセージ中のファイル識別情報で特定されたユーザ情報について、他人の利用を阻止するためのデータ処理を施すことを特徴とする請求項９～請求項１４の何れかに記載の携帯端末情報保護方法。

【請求項１７】前記情報保護命令メッセージを受信した携帯端末が、保護対象となった前記所定のユーザ情報を上記セキュリティ制御装置に送信した後、他人の利用を阻止するためのデータ処理を施すことを特徴とする請求項９～請求項１６の何れかに記載の携帯端末情報保護方法。

【請求項１８】前記情報保護命令メッセージを受信した携帯端末が、保護対象となった前記所定のユーザ情報を上記メッセージ中で指定された暗号鍵によって暗号化した形で上記セキュリティ制御装置に送信することを特徴とする請求項１７に記載の携帯端末情報保護方法。

【請求項１９】前記情報保護命令メッセージを受信した携帯端末が、保護対象となった前記所定のユーザ情報を消去することによって、他人の利用を阻止することを特徴とする請求項９～請求項１８の何れかに記載の携帯端末情報保護方法。

【請求項２０】前記情報保護命令メッセージを受信した携帯端末が、保護対象となった前記所定のユーザ情報にデータ変換を施すことによって、他人の利用を阻止することを特徴とする請求項９～請求項１８の何れかに記載の携帯端末情報保護方法。

【請求項２１】前記セキュリティ管理データの前記セキュリティ制御装置への登録が、保護対象となる携帯端末から無線ネットワークを介して行われることを特徴とする請求項９～請求項２０の何れかに記載の携帯端末情報保護方法。

【請求項２２】前記セキュリティ制御装置への情報保護要求が、電話を利用して行われることを特徴とする請求項９～請求項２１の何れかに記載の携帯端末情報保護方法。

【請求項２３】携帯端末と、無線ネットワークと、上記無線ネットワークに接続されたセキュリティ制御装置とからなり、
上記セキュリティ制御装置が、携帯端末に関するセキュリティ管理データを記憶するための記憶手段と、紛失状態にある携帯端末の所有者からのデータ保護要求に応じて、上記セキュリティ管理データに基づいてデータ保護命令メッセージを生成し、これを上記無線ネットワークを介して該当携帯端末に送信するためのメッセージ生成送信手段を備え、
上記セキュリティ制御装置にセキュリティ管理データを登録済の携帯端末が、上記無線ネットワークと通信するための無線通信手段と、データ処理手段と、上記無線通信手段で受信したデータ保護命令メッセージに応答して上記データ処理手段によって実行すべき専用ソフトウエアとを備え、上記専用ソフトウエアの実行によって、上記携帯端末内の特定のデータを無効化するようにしたことを特徴とする携帯端末の情報保護システム。

【請求項２４】前記セキュリティ制御装置が、前記携帯端末所有者からのデータ保護要求時に、上記所有者が提示した個人認証情報と前記セキュリティ管理データとして予め登録されている個人認証情報とに基づいて上記保護要求の受け付け可否を判定する判定手段を備え、受付可と判断されたデータ保護要求について前記データ保護命令メッセージの生成と送信を行うことを特徴とする請求項２３に記載の携帯端末の情報保護システム。

【請求項２５】前記セキュリティ制御装置のメッセージ生成送信手段が、前記データ保護命令メッセージ中に前記セキュリティ管理データで予め登録されている個人認証情報を含めた形でメッセージを送信し、
前記携帯端末が、受信したデータ保護命令メッセージに含まれる個人認証情報と予め該携帯端末に記憶されてい

5

る個人認証情報とに基づいて、上記データ保護命令メッセージへの応答可否を判定する判定手段を備え、
上記判定手段で応答可と判断されたデータ保護命令メッセージに応答して、前記特定のデータについてのデータ処理を実行するようにしたことを特徴とする請求項２３または請求項２４に記載の携帯端末の情報保護システム。

【請求項２６】前記携帯端末の無線通信手段が、前記データ保護命令メッセージを識別し、前記データ処理手段の電源を自動的に投入するための電源制御手段を備えることを特徴とする請求項２３～請求項２５の何れかに記載の携帯端末の情報保護システム。

【請求項２７】前記携帯端末の専用ソフトウエアが、前記特定のデータについて、前記セキュリティ制御装置に転送した後、データ消去またはデータ暗号化によって他人に対するデータ無効化を行うことを特徴とする請求項２３～請求項２６の何れかに記載の携帯端末の情報保護システム。

【請求項２８】前記携帯端末が、前記セキュリティ制御装置への転送データを暗号化するための手段を備えることを特徴とする請求項２７に記載の携帯端末の情報保護システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、携帯端末および携帯端末情報保護方法に関し、更に詳しくは、マイクロプロセッサとメモリ手段と無線通信手段とを備えた可搬型端末、およびメモリに蓄積されたユーザ情報の保護方法に関するのものである。

【０００２】

【従来の技術】半導体メモリやマイクロプロセッサ等の電子技術の向上によって、ノート型のパーソナルコンピュータの他に、電子手帳、パーソナルデジタルアシスタンツ（Personal Digital Assistants：ＰＤＡ）、新携帯情報ツールなどと呼ばれる携帯端末装置が実用化されている。特に小型化、軽量化された携帯端末装置は、上着のポケットなどに入れて容易に持ち運ぶことができ、移動途中でデータの入出力操作をしたり、通信機能を利用して出先からオフィス側の情報処理システムとデータ交信する等、利用形態も多様化している。

【０００３】然るに、これらの携帯端末装置は、所有者本人によってオフィス外に持ち出され、また、鞄やポケット等に入れ持ち運ばれるため、移動途中で盗難に遭遇したり、不注意による紛失、置き忘れ等、本人の意に反した形で他人の手に渡る機会が増え、端末装置内に記憶された情報が第三者に参照、悪用される危険性が高まってきている。従来、秘密性の高い情報を保護するための方法として、アクセスを制限すべき情報ファイルにはパスワードを対応付けておき、利用者がこの情報ファイルを参照しようとすると、システム側からパスワードの入力を促し、入力されたパスワードが予め登録されている正規のものと一致した場合にのみ、アクセスを許容する方法が知られている。

6

【０００４】

【発明が解決しようとする課題】携帯端末は、主として個人の所有物として利用され、オフィス内に設置された固定端末のように不特定の複数の利用者が共用したり、他人に貸し借りすることを前提としたものではない。このため、携帯端末の所有者は、端末が自分の管理下にある間は、携帯端末内にあるユーザ情報の保護について意識することは稀である。また、携帯端末の所有者は、携帯端末の蓄積情報を自分の所有物として気軽に扱うことを望み、他人に見られてはならない情報であっても、平常時には、手続き的に面倒な上述したパスワード等による秘密保護策はとらず、必要な情報を随時、迅速にアクセスできる操作環境で端末を利用することが多い。携帯端末の所有者が、端末内の蓄積情報について他人による参照と利用を是非とも避けたいと意識するのは、自分の端末が紛失したことに気付いた時である。

【０００５】本発明の目的は、端末を紛失した時、該端末内に残された所有者にとって重要な情報が第三者に悪用されるのを防止できるようにした携帯端末装置、端末情報の保護方法および端末情報保護システムを提供することにある。本発明の他の目的は、端末を紛失した時、該端末内に残された所有者にとって重要なユーザ情報を所有者の手元に回収できるようにした携帯端末装置、端末情報の保護方法および端末情報保護システムを提供することにある。本発明のさらに他の目的は、通常時において端末内の蓄積情報へのアクセスが容易であり、端末紛失時に該端末内に残された所有者にとって重要なユーザ情報を保護できるようにした携帯端末装置、端末情報の保護方法および端末情報保護システムを提供することにある。

【０００６】

【課題を解決するための手段】上記目的を達成するため、本発明の携帯端末情報保護方法および保護システムでは、携帯端末に格納されているユーザ情報を保護するために必要なセキュリティ管理データを無線ネットワークに接続されたセキュリティ制御装置に予め登録しておき、携帯端末の紛失に気付いた端末所有者が、上記セキュリティ制御装置に対して自分の携帯端末についての情報保護を要求すると、セキュリティ制御装置が、予め登録してあるセキュリティ管理データに基づいて情報保護命令メッセージを生成し、これを無線ネットワークを介して携帯端末に送信し、上記情報保護メッセージを受信した携帯端末が、端末内に保持する所定のユーザ情報について他人の利用を阻止するためのデータ処理を施すようにしたことを特徴とする。

【０００７】本発明の実施例によれば、上記セキュリティ制御装置が、目的の携帯端末が無線ネットワークによ

る通信が可能な状態にあるか否かをチェックし、通信可能な状態にあることを確認して上記情報保護命令メッセージを送信し、もし通信不能な状態であれば、通信可否の確認を所定の繰返しパターンで繰り返すようにしている。上記情報保護命令メッセージの送信に先立って、上記セキュリティ制御装置が、無線ネットワークにおける移動端末データを管理する管理装置に対して目的携帯端末の状態を問合せ、上記移動端末データ管理装置が、セキュリティ制御装置に上記携帯端末の位置登録の有無を通知し、もし、位置登録されていなかった場合には、上記携帯端末について状態問合せを受けたことを記憶しておき、当該携帯端末が位置登録された時点で上記セキュリティ制御装置に通知するようにし、上記セキュリティ管理装置が、移動端末データ管理装置からの通知に応じて情報保護命令メッセージを送信するようにしてもよい。

【０００８】本発明において、上記セキュリティ管理データは、例えば、携帯端末のアドレス情報（無線ネットワークにおけるアドレスまたは電話番号）と、登録者識別情報と、登録者認証情報と含む。このような管理データを予めセキュリティ制御装置に登録しておくことによって、情報保護の要求時に、要求者（紛失した携帯端末の所有者）に自分の識別情報と認証情報を提示させ、セキュリティ制御装置が、上記提示された情報と、セキュリティ管理データとして既に登録済の情報とを照合して要求者の正当性をチェックし、正当性が確認された場合に限り、上記情報保護命令メッセージの生成と送信を行わせるようにすることができる。また、携帯端末に送信する情報保護命令メッセージに上記認証情報を設定しておき、上記情報保護命令メッセージを受信した携帯端末に、受信メッセージから抽出した認証情報と携帯端末内に予め設定されている認証情報とに基づいて上記受信メッセージの正当性をチェックさせ、正当性が確認された場合に限り、情報保護のためのデータ処理を実行させることができる。

【０００９】本発明による携帯端末は、無線通信手段と、出力手段と、入力手段と、ユーザデータを蓄積するためのメモリ手段と、上記入力手段からのユーザ操作入力に応じて、上記メモリ手段へのユーザデータの書込み、読み出し、上記出力手段への情報出力、および上記無線通信手段を介して他装置との情報の交信を行うためのデータ処理手段とからなる携帯端末装置において、上記メモリ手段に記憶されているデータについての情報保護要求者を認証するための認証情報を記憶する手段と、上記無線通信手段によって受信された情報保護命令メッセージに含まれる認証情報と上記記憶手段に予め記憶してある認証情報との対応関係から情報保護要求の正当性をチェックし、正当性が確認された場合に、上記メモリ手段に蓄積されている特定のユーザデータを無効化するための所定のデータ処理手順を記述した情報保護用ソフトウエアとを備え、上記データ処理手段が、上記無線通信手段からの通知に応答して上記情報保護用ソフトウエアを実行し、上記特定のユーザデータを無効化して他人による利用を阻止するようにしたことを特徴とする。

【００１０】保護すべきユーザデータを特定するために、本発明の携帯端末では、例えば、メモリ手段を一般情報領域と保護情報領域とに分けておき、情報保護上記保護情報領域に蓄積されているユーザデータについて無効化する。この代わりに、情報保護用ソフトウエアが、保護対象とすべきユーザデータのファイル識別情報を予め保持し、上記ファイル識別情報で特定されたユーザデータを無効化するようにしてもよい。ユーザデータの保護形態として、上記情報保護用ソフトウエアにより、ユーザデータ無効化に先立って、ユーザデータを他の装置、例えば、上記情報保護要求メッセージの送信元に転送し、後で端末所有者の手元に回収できるようにしてもよい。この場合、上記ユーザデータを暗号化して転送するようにしてもよい。

【００１１】

【発明の実施の形態】図１は、無線ネットワークを利用した本発明による携帯端末情報の保護方法を実現するためのシステム全体構成を示す。図において、１は、有線網５を介して相互接続された複数の無線基地局１２（１２Ａ～１２Ｎ）と移動端末制御データを格納したデータベースシステム１１とからなる無線ネットワーク、１０は上記無線ネットワークに接続されたセキュリティコントローラ（セキュリティサーバ）である。１４（１４Ａ～１４Ｍ）は上記無線ネットワークを利用する移動端末であり、通常の移動電話機の他に、本発明が対象とする携帯情報端末（以下、単に携帯端末という）もこれらの移動端末の一種となる。以下の実施例では、無線ネットワーク１としてＰＨＳ(Personal Handy-phoneSystem)を適用した場合について説明する。有線網５には、図示しない交換機システムを介して、固定端末１８や他の公衆電話通信網が接続される。但し、上記無線ネットワーク１には、携帯端末とセキュリティコントローラとの間で計算機コマンドおよびデータを含むメッセージの通信を可能とする他の方式のものを適用してもかまわない。

【００１２】上記データベースシステム（ＰＨＳシステムＤＢ）１１には、移動端末制御データとして、移動端末（ＰＨＳ電話機およびＰＨＳ機能内蔵の携帯端末）の位置情報や認証情報などが管理され、本実施例では、セキュリティコントローラ１０は上記データベースシステムと結合されている。セキュリティコントローラ１０は、携帯端末１４の所有者からのセキュリティ登録要求に応じて、携帯端末１４の情報保護に必要なセキュリティ管理データを登録しておき、電話１８等の通信装置を介してユーザから携帯端末情報の保護要求を受けたとき、予め登録されているセキュリティ管理データに基づいて、ユーザの認証、携帯端末の特定を行い、無線ネッ

トワークシステムを介して、後述する目的端末の現在位置情報の入手と情報の保護動作を行う。携帯端末１４の位置情報は、ＰＨＳシステムＤＢ１１をアクセスすることにより得られ、情報保護は、携帯端末１４に情報保護命令を送信し、携帯端末に内蔵されている情報保護プログラムを実行させることにより実現する。

【００１３】図２は、携帯端末の所有者によるセキュリティコントローラ１０への情報保護登録の手順を示す。携帯端末１４で登録操作５７を行うと、セキュリティコントローラ１０と接続され、セキュリティコントローラ１０に登録要求５１が送信される。セキュリティコントローラ１０は、上記登録要求５１に応答して登録受付動作６１を実行し、要求元の携帯端末１４に登録情報要求５２を送付する。携帯端末１４は、上記登録情報要求に応じて、所有者に情報保護に必要な情報を入力させ、これを登録情報５３としてセキュリティコントローラ１０に送信する。セキュリティコントローラ１０は、上記登録情報５３を解析した後、登録情報確認要求５４を携帯端末４に送信する。所有者が、登録内容に誤りのないことを確認すると、登録確認応答５５が携帯端末１４からセキュリティコントローラ１０に送付される。セキュリティコントローラ１０は、上記登録確認応答を受信すると、登録情報確認動作６３を実行し、登録情報５３を登録データテーブルに登録し、携帯端末１４に登録ＯＫレスポンス５６を送信して登録処理を終了する。同様に、携帯端末側でも、上記登録ＯＫレスポンス５６を受信し、これをユーザが確認して登録処理を終了する。

【００１４】図３は、携帯端末とセキュリティコントローラとの間で通信される携帯端末情報保護用のメッセージフォーマット７０を示す。メッセージ７０は、システムＩＤ７１、動作ＩＤ７２、データ量７３、データ内容７４、およびＣＲＣ（サイクリック・リダンダンシー・チェック）７５の５つのフィールドからなる。システムＩＤ７１には、このメッセージが携帯端末情報保護用のものであることを示すコードが設定される。動作ＩＤ７２は、このメッセージの種類を示し、登録要求５１、登録情報要求５２等を識別するための識別子が設定される。データ量７３は、後続するデータ内容フィールド７４のデータ量をバイト単位で示し、ＣＲＣ７５は、動作ＩＤフィールド７２からデータ内容フィールド７４までのデータ誤りチェックに利用される。

【００１５】登録要求５１に応答してセキュリティコントローラ１０から携帯端末に送信される登録情報要求メッセージ５２のデータ内容７４は、データフォーマット７６で示すように、必要データひな型７９と暗号鍵Ａ：８０とを含む。必要データひな型７９は、登録情報５３として必要な情報項目を携帯端末所有者に表示するためのデータであり、入力すべき情報項目を表す文字列とそのバイト長とで構成されている。暗号鍵Ａ：８０は、例えば、公開暗号鍵方式における公開暗号鍵であり、携帯端末１４は、登録情報５３を上記暗号鍵Ａを用いて暗号化した形で、セキュリティコントローラに送信する。

【００１６】登録情報メッセージ５３のデータ内容７４は、データフォーマット７７で示すように、携帯端末識別ＩＤ８１、携帯端末電話番号８２、登録者ＩＤ８３、認証情報８４、処理番号８５、および暗号鍵Ｂ：８６を含む。携帯端末識別ＩＤ８１は、携帯端末のシリアルナンバーであり、セキュリティコントローラが携帯端末と通信する際に、正しい携帯端末と通信しているか否かの判定に用いられる。携帯端末電話番号８２は、携帯端末が内蔵するＰＨＳの電話番号であり、セキュリティコントローラ１０は、この電話番号によって、紛失状態にある携帯端末を呼び出す。登録者ＩＤ８３は、携帯端末所有者のＩＤであり、セキュリティコントローラは、携帯端末情報保護サービスの実行に際して、このＩＤで利用者とセキュリティ管理データを特定する。認証情報８４は、携帯端末情報保護サービスの要求者が登録者本人か否かを確認するための暗証情報（パスワード）である。処理番号８５は、端末情報保護の形態を示す。例えば、端末が保持する情報（保護情報）を消去する場合は「処理番号＝１」、保護情報をセキュリティコントローラ側に回収（転送）した後、端末の保持する情報を消去する場合は「処理番号＝２」、の如く端末情報保護の形態（種類）をコード化しておき、端末所有者は、登録時に予め情報保護の形態を指定しておく。暗号鍵Ｂ：８６は、公開暗号鍵方式の公開暗号鍵であり、セキュリティコントローラから携帯端末に送信する情報を暗号化するために用いられる。

【００１７】登録ＯＫレスポンス５６のデータ内容７４は、データフォーマット７８に示すように、登録者ＩＤ８３と処理番号８５を含む。処理番号８５は、上記登録情報メッセージ５３において利用者が指定し、セキュリティコントローラ側で受け付けられた処理番号を示す。

【００１８】図４は、登録手続きのために携帯端末に表示されるデータ入力画面の１例を示す。９０は登録開始画面、９１は登録情報入力画面、９２は所有者確認画面であり、端末所有者は、表示内容に従って順次にデータを入力する。登録開始画面９０において、メニュー９３から「セキュリティ登録」を選択すると、登録ウィンドウ９４が表示される。登録ウィンドウ９４には、端末紛失時の情報保護を要求するとき使用する非常時連絡先電話番号と、情報登録処理の実行要否を指示するための「ＹＥＳ（はい）」、「ＮＯ（いいえ）」のボタンが用意されている。情報登録処理を実行しようとする端末所有者は、上記非常時連絡先電話番号を手帳等にメモした後、「ＹＥＳ（はい）」ボタンを選択する。この操作によって、携帯端末からセキュリティコントローラ１０へ自動的にダイヤルされ、コネクションが確立されると、携帯端末からセキュリティコントローラ１０に登録要求５１が送信される。なお、上記自動ダイヤルされる電話

番号は、上記非常時連絡先電話番号とは別のものとする。また、上記非常時連絡先電話番号は、携帯端末にロードされる情報保護用のソフトウエアの説明書で確認するようにしてもよい。

【００１９】登録情報入力画面９１は、登録情報要求メッセージ５２でセキュリティコントローラ１０から送信された必要データひな形７９に基づいて構成される登録情報入力ウィンドウ９５を有し、端末所有者は、このウィンドウで登録情報（セキュリティ管理データレコード）として必要な複数項目のデータを入力する。全てのデータ項目の入力を終え、所有者が送信ボタンを選択すると、データ内容７４としてデータフォーマット７７の内容をもつ登録情報メッセージ５３が生成され、セキュリティコントローラ１０に送付される。ユーザ確認画面９２は、セキュリティコントローラ１０から登録ＯＫレスポンス５６を受信した時、携帯端末に表示される画面であり、終了ボタンと登録情報を含むユーザ確認ウィンドウ９６が表示される。所有者が、終了ボタンを選択すると登録処理が終了する。このとき、セキュリティ管理データの一部、例えば、登録者ＩＤとパスワードは、携帯端末内の不揮発性メモリに記憶保持される。

【００２０】図５は、登録処理時にセキュリティコントローラ１０が実行する処理プログラムのフローチャートの１例を示す。ブロック６１、６２、６３は、それぞれ図２に示した登録受付動作６１、登録情報受付動作６２、登録情報確認動作６３に対応している。セキュリティコントローラ１０は、携帯端末からの着信待ち状態（ステップ１０１）にあり、着信がなければ、常駐処理（１０２）によって待ち状態を繰り返す。メッセージが受信されると、メッセージデータ（入力データ）をチェック（１０３）し、受信メッセージが登録要求５１か否かを判定する（１０４）。登録要求５１であれば、登録情報要求データ５２を作成し、携帯端末に送信（１０６）した後、次のメッセージの受信を待つ（１０７）。上記最初のメッセージが登録要求５１でなければ、その他の処理１０５を行う。

【００２１】次のメッセージとして暗号鍵Ａで暗号化された登録情報５３を受信すると、上記暗号鍵Ａと対応する秘密暗号鍵を適用して登録情報をで解読、解析（１０８）した後、登録情報確認要求メッセージ５４を作成して、携帯端末に送信（１０９）し、次のメッセージの受信を待つ（１１０）。上記登録情報確認要求メッセージ５４のデータ内容７４には、セキュリティコントローラ１０が受信した登録情報メッセージ５３のデータ内容７７を含む。携帯端末からの登録確認応答５５を受信すると、既に受信済の登録情報をセキュリティ管理データとして登録（１１３）し、登録ＯＫレスポンスを作成して携帯端末に送信する（１１４）送付する。なお、携帯端末側から登録確認応答５５として、登録情報メッセージ５３と同様のデータ内容を持つメッセージを送信させ、破線で示すように、受信登録確認応答メッセージ５５のデータ内容を解読、解析した後、既に受信済の登録情報と比較し（１１２）、一致した場合に登録処理（１１３）し、不一致の場合は、登録情報要求ステップ（１０６）から再実行するようにしてもよい。

【００２２】図６は、紛失した携帯端末の所有者から、例えばブッシュホン（電話機）によって非常時連絡先電話番号をダイヤルし、セキュリティコントローラ１０に情報保護を要求した場合の保護システムの動作手順を示す。ここでは、上記情報保護の要求を受け付けた時点で、紛失携帯端末がＰＨＳシステムと通信可能な状態にあり、セキュリティコントローラ１０が紛失携帯端末のアクセスに成功した場合の動作例を示す。また、図６における動作Ｓ１：１３４～Ｓ５：１３８、および後述する図７における動作Ｓ６：１５８～Ｓ７：１５９を実行するセキュリティコントローラ１０の動作フローチャートを図１０に示し、以下図１０の動作ステップも参照して動作説明する。

【００２３】携帯端末の紛失に気付いた所有者が、電話機１８で非常時連絡先の電話番号をダイヤルすると（動作Ｕ１：１３１）、セキュリティコントローラ１０との間にコネクションが確立する。この場合、発呼時に電話機から発信される呼制御信号が保護要求１２１となる。セキュリティコントローラ１０側では、上記非常時電話番号への着信は、音声応答システムに接続され、最初の自動応答メッセージ（認証確認メッセージ）１２２として、例えば、「登録者ＩＤと＃、それに引き続いてパスワードと＃を押してください」という内容の音声メッセージを出力する（動作Ｓ１：１３４、図１０のステップ１０１～２０５）。所有者は、上記音声メッセージに答えて、数字キーと＃ボタンを用いて、登録者ＩＤとパスワードを入力する（動作Ｕ２：１３２）。これらの入力データは、認証データ１２３として送信される。

【００２４】セキュリティコントローラ１０は、上記認証データ１２３を受信すると、登録者ＩＤと同一のＩＤをもつ登録済のセキュリティ管理データレコードを検索し、受信したパスワードが登録済の認証情報８４と一致するか否かを判定し、情報保護の要求者が登録された人物である事を確認した後、要求確認メッセージ１２４を出力する（動作Ｓ２：１３５、図１０のステップ２０６～２０８）。上記要求確認メッセージ１２４は、例えば、「只今から情報保護動作を開始します。携帯端末が発見できなかった場合、引き続いて、探索動作を続けます。すぐに見つからない場合は、後日、連絡します。連絡先の電話番号と＃ボタンを押して、しばらくお待ちください。」のような内容とする。

【００２５】所有者が、電話番号入力と＃ボタン操作（動作Ｕ３：１３３）行うと、セキュリティコントローラは、ＰＨＳシステムＤＢ１１に対して、セキュリティ管理データレコードで登録されているＰＨＳ電話番号を

指定して、携帯端末検索要求１２７を送信する（動作Ｓ３：１３６、図１０のステップ２０９～２１１）。ＰＨＳシステムＤＢ１１は、上記検索要求（１２７）を受信すると、データベースから該当するＰＨＳ電話番号を持つ携帯端末が位置登録されているかを検索し、その結果を携帯端末検索レスポンス１２８として、セキュリティコントローラ１０に送信する（動作Ｎ１：１３９）。

【００２６】セキュリティコントローラ１０は、目的携帯端末が位置登録されている場合、その携帯端末に、予め登録してあった処理番号８５で情報保護の種類を指定した形で、情報保護命令１２９を送信する（動作Ｓ４：１３７、図１０のステップ２１２～２１４）。上記情報保護命令１２９を受信した携帯端末１４は、情報保護プログラムを実行し、これが完了すると、必要に応じて保護データを伴う保護終了報告１３０をセキュリティコントローラ１０に送信する（動作Ｐ１：１４０）。

【００２７】セキュリティコントローラ１０は、上記保護終了報告１３０を受信すると、退避すべき保護データがなければ直接、もしあれば、これを上記セキュリティ管理データレコードと対応付けて蓄積（退避データ記録）した後、情報保護の終了通知１２６を回答（動作Ｓ５：１３８、図１０のステップ２１５～２０８）し、手続きを終了する。上記情報保護の終了通知１２６は、例えば、「携帯端末の情報の保護を完了しました。」の内容をもつ音声メッセージであり、保護データを回収した場合は、その旨を示す音声メッセージを追加する。

【００２８】尚、上記実施例において、ＰＨＳシステムＤＢに対する携帯端末検索要求動作Ｓ３とその応答動作Ｎ１は、上記携帯端末検索要求１２７に応答して、ＰＨＳシステムＤＢが、目的携帯端末が位置登録されている基地局を見つけ出し、この基地局の識別子と対応関係にある基地局所在地（住所）情報を検索し、例えば、上記基地局所在地を中心としたセル半径でもって目的携帯端末の概略的な現在位置を表し、これを上記携帯端末検索レスポンス１２８によってセキュリティコントローラに通知し、セキュリティコントローラが、上記現在位置情報を検索要求者に通知する場合に有効となる。また、図８で説明するように、携帯端末の所有者が情報保護を要求した時点で携帯端末が通信不能の状態にあった場合に、この端末が無線ネットワークに位置登録したのを検出して、自動的に情報保護命令を発行する場合に有効となる。

【００２９】もし、このような端末所有者への端末位置情報サービスを全く必要としない場合は、ＰＨＳシステムＤＢへの端末検索要求１２７を省略し、目的携帯端末が位置登録されているか否かに無関係に、セキュリティコントローラ１０が、上記動作Ｓ３において目的端末への呼（コネクション）設定を試み、コネクションが設定された場合に動作Ｓ４を実行するようにしてもよい。目的端末が通信不能の状態にあった場合は、セキュリティコントローラ１０が、所定の繰返しパターンで自動的に発呼を繰返すようにすればよい。

【００３０】図７は、図６で示した情報保護の要求を受け付けた時点で、紛失携帯端末を発見できなかった場合の動作例を示す。図７の動作シーケンスで、ＰＨＳシステムＤＢ１１がセキュリティコントローラ１０に携帯端末検索レスポンス１２８を送信するまでの手順は図６と同様である。この場合、セキュリティコントローラ１０から検索要求のあった携帯端末の現在位置確認に失敗した場合、ＰＨＳシステムＤＢ１１側で、上記携帯端末の情報レコードに、セキュリティコントローラ１０で探索中の端末である旨を示すフラグをたてておくとよい。この例では、セキュリティコントローラ１０は、ＰＨＳシステムＤＢ１１から位置確認失敗を示す携帯端末検索レスポンス１２８を受信し、動作Ｓ４：１３７において、所有者に、例えば、「お捜しの携帯端末が見つかりません。引き続いて端末の監視を行いますが、ここで端末捜査と情報保護を打ち切る場合は２＃を、継続する場合１＃を押してください。」の内容をもつ音声メッセージ（常駐確認メッセージ）１５１を送信する（図１０のステップ２１９）。

【００３１】所有者が「２＃」を選択した場合は、セキュリティコントローラ１０は、「これでサービスを終了させて頂きます。」の音声メッセージを出力して（動作Ｓ６：１５８、図１０のステップ２２０、２２１、２２７）、通信を終了する。所有者が「１＃」を選択した場合は、上記動作Ｓ６：１５８で、例えば、「お客様の連絡先電話番号は、ＸＸＸＸＸＸＸＸＸＸで間違いないでしょうか。宜しければ１＃、電話番号を変更する場合は２＃を押し、再度、電話番号を入力した後、＃を押してください。」の内容の音声メッセージ（連絡先確認メッセージ）１５３を送信する（図１０のステップ２２１、２２２）。所有者が、上記確認メッセージに応答操作（動作Ｕ６：１５７）すると、セキュリティコントローラは、上記応答操作による連絡先レスポンス１５４の内容を解析し、「１＃」の場合は、例えば、「これでサービスを終了させて頂きます。」の内容をもつ終了メッセージ１５５を送信した後、通信を終了する。もし、上記確認メッセージに応答して「２＃」と電話番号が入力された場合は、再度、電話番号確認メッセージを送信した後、同様の動作を繰り返す（動作Ｓ７：１５９、図１０のステップ２２３～２２７）

図８は、紛失した携帯端末を自動的に見つけ出すための常駐保護処理の動作手順を示す。また、図１１に、上記図８中の動作Ｓ８：１６６とＳ９：１６７と対応するセキュリティコントローラ１０の動作フローチャートを示し、以下図１１も参照して動作説明する。紛失した携帯端末１４の電源がＯＮになると、内蔵ＰＨＳ電話機能によって、基地局に位置登録要求１６１が発信され、ＰＨＳシステムＤＢ１１が端末の位置登録（動作：１６８）

を行う。ＰＨＳシステムＤＢ１１は、何れかの基地局から位置登録情報１６１を受信すると、位置登録の動作過程で、上記携帯端末の情報レコード中に、セキュリティコントローラ１０で探索中の端末である旨を示すフラグを見つけ、セキュリティコントローラ１０に対して、紛失端末位置を示す位置登録通知１６２を送信する。

【００３２】セキュリティコントローラ１０は、ＰＨＳシステムＤＢからの位置登録通知の受信待ち状態（図１１のステップ１０１）にあり、上記位置登録通知１６２を受信すると、紛失携帯端末１４に対して、ＰＨＳ電話システムによる通信を開始し、情報保護命令１２９を送信する（動作Ｓ８：１６６、図１１のステップ２４３～２４５）。携帯端末１４は、上記情報保護命令１２９に応答して、図６で示したのと同様に情報保護プログラムを実行し、保護終了報告１３０をセキュリティコントローラ１０に送信する。セキュリティコントローラ１０は、上記保護終了報告１３０を受信すると、動作Ｓ９：１６７において、もし、保護データがあればこれを蓄積（避難データ記録し（図１１のステップ２４６～２４８）、セキュリティ管理データレコードに情報保護終了を記録した後、上記データレコードに記憶してある端末所有者の連絡先に自動的ダイヤルし、情報保護の報告１６５を音声メッセージで通知する（図１１のステップ２４９～２５１）。上記実施例では、保護要求のあった携帯端末が位置登録をした時点で、ＰＨＳシステムＤＢ１４が、情報保護要求の有無をチェックし、自動的にセキュリティコントローラに通知する方式となっているが、ＰＨＳシステムＤＢ１４にこのような特殊な機能を付加したくない場合は、セキュリティコントローラ１０が、定期的に携帯端末に発呼を繰り返すことによって、動作８：１６６の切っ掛けを得るようにすればよい。

【００３３】図９は、上述した情報保護動作の実行時に携帯端末、セキュリティコントローラ、ＰＨＳシステムデータベース間で通信するメッセージ７０のフォーマットの一例を示す。メッセージフォーマット７０の基本構造は、図３に示したものと同様で、データ内容７４がメッセージ種類によって異なっている。３０１は、図６及び図７で示した携帯端末検索要求メッセージ１２７のデータ内容を示す。処理命令メッセージ３０５と携帯端末電話番号７９の２つのフィールドからなり、上記処理命令メッセージ３０５には、ＰＨＳシステムＤＢ１１に対する要求内容を示す文字列が設定され、携帯端末電話番号７９には、検索対象となる携帯端末のＰＨＳ電話番号が設定される。

【００３４】３０２は、図６及び図７で示した携帯端末検索レスポンス１２８と、図８で示した位置登録通知１６２に用いるメッセージのデータ内容７４を示す。データ内容は、携帯端末の有無３１０、携帯端末電話番号８２、位置情報３０６の３つのフィールドからなり、携帯端末電話番号８２には、検索対象となった携帯端末のＰＨＳ電話番号が設定され、位置情報３０６には、上記携帯端末が位置するＰＨＳシステム内の接続ポイント（基地局）を示す位置情報が設定され、この位置情報によって、携帯端末の概略的な現在位置を知ることができる。

【００３５】３０３は、図６および図８で示した情報保護命令１２９のメッセージにおけるデータ内容７４を示し、携帯端末識別ＩＤ８１、携帯端末電話番号８２、登録者ＩＤ８３、認証情報８４、処理命令３１１および暗号鍵Ｃ：３０７を含む。携帯端末識別ＩＤ８１、携帯端末電話番号８２、登録者ＩＤ８３、認証情報８４、処理番号８５は、セキュリティ管理データとして登録されたものであり、情報保護命令１２９を受信した時、携帯端末１４側で、受信メッセージの信頼性をチェックするために利用される。暗号鍵Ｃ３０７は、公開暗号鍵方式の公開暗号鍵であり、携帯端末は、この暗号鍵Ｃを用いてセキュリティコントローラに送信する保護情報を暗号化する。

【００３６】３０４は、図６及び図８に示した保護終了報告１３０のメッセージにおけるデータ内容７４を示し、メッセージ種別ＩＤ３０８とデータ３０９の２つのフィールドからなる。メッセージ種別ＩＤ３０８は、これに続くデータフィールド３０９に、例えば、保護終了報告コードのみを含む場合は「０」、保護終了報告コードと保護データとを含み上記保護データに続きがない場合には「１」、保護データに続きデータがある場合は「２」が設定される。データフィールド３０９に内容は、暗号鍵Ｃ３０７を用いて暗号化されている。

【００３７】図１２は、図６、図７、図８における動作Ｎ１：１３９、Ｎ２：１６８を実行するＰＨＳシステムＤＢの動作フローチャートを示す。ＰＨＳシステムＤＢ１１は、受信メッセージをチェックし（ステップ２６１）、受信メッセージが携帯端末からの位置登録要求であれば、動作Ｎ２：１６８を実行する。この場合、通常の位置登録動作を行い（ステップ２７１）、もし、その携帯端末についてセキュリティーコントローラから探索要求がなされいることが判明すると、セキュリティコントローラ宛の通知情報（図８の位置通知１６２）を作成し（２７２）、セキュリティコントローラへ送信（２７３）した後、メッセージ受信待ち状態に戻る。

【００３８】セキュリティコントローラから携帯端末検索要求１２７を受信した場合は、動作Ｎ１：１３９を実行する。この場合、先ず、携帯端末検索要求を解析し（２６４）、検索要求で指定されている携帯端末電話番号（図９に示されている携帯端末電話番号７９）に基づいてデータベース情報を検索し（２６５）、目的端末が位置登録されているか否かをチェックする（２６６）。目的端末が位置登録されていた場合は、図９に示したデータ内容フォーマット３０２におけるフィールド３１０に携帯端末有りを示す「１」、フィールド８２に目的携帯端末の電話番号、フィールド３０６に上記目的携帯端

末を収容している基地局情報が設定された応答メッセージ１２８を作成し（２６７）、セキュリティコントローラに送信する（２７０）。目的携帯端末の位置が未登録の場合、上記フィールド３１０と３０６の「0」が設定された応答メッセージ１２８を作成し（２６８）、これをセキュリティコントローラに送信する（２７０）。

【００３９】図１３は、本発明が適用される携帯端末におけるデータ保護動作Ｐの詳細を示す１フローチャートである。携帯端末は、通常のデータ処理動作状態２８２において通信制御部から割り込みを受けた場合（２８１）、携帯端末のＲＯＭに格納されているデータ保護に専用ソフトウェアを起動し、通信メッセージを解析する（２８４）。ＰＨＳ電話機能および通信制御部が受信待ち状態にあり、ＣＰＵ本体部の電源が未投入状態にある場合は、ＣＰＵ電源を自動的に投入した後、上記通信メッセージの解析を行う。

【００４０】上記割込み原因となった通信制御部での受信メッセージがセキュリティコントローラからの情報保護命令１２９であれば、図３で説明したように、データ部が暗号鍵Ｂ：８６で暗号化されているため、その場合は、暗号鍵Ｂに対応して予めＲＯＭに記憶されている秘密鍵を用いてメッセージ内容を解読する。上記通信内容が情報保護命令１２９でなければ（２８４）、通常の通信処理（２８２）を行い、情報保護命令の場合は、認証チェックを行う（２８６）。認証チェックは、上記情報保護命令中に含まれる認証情報（図９におけるフィールド８５の内容）と、携帯端末情報保護の登録時に携帯端末内に記憶しておいた正当な所有者の認証情報（パスワード）とを比較することによって行う。認証結果に問題があれば以降の処理を省略して最初のステップ２８１へ戻る。

【００４１】認証に問題がなければ、保護命令の内容を解析し（２８７）、処理番号フィールド８５の値からデータ転送の要否を判定し（２８８）、データ転送の必要がなければステップ２９１へ進む。データ転送の必要があれば、情報保護命令中の暗号鍵（暗号鍵Ｃ：３０７）を用いて端末情報（保護データ）を暗号化し（２８９）、暗号化された端末情報をセキュリティコントローラへ送信（２９０）した後、ステップ２９１に進む。ステップ２９１では、端末情報の機密保護（無効化または書き換え）処理を行う（２９１）。データ機密保護は、例えば、端末情報のメモリ消去、または偽データへの変換によって達成する。データ機密保護が終了すると、データ保護終了メッセージをセキュリティコントローラへ送信し（２９２）、割り込み処理を終了し、元の状態に戻る。

【００４２】図１４は、セキュリティコントローラ１０の構成を示す。セキュリティコントローラ１０は、ＣＰＵ２０、ＲＯＭ２１、ＲＡＭ２２、データファイル２３、通信制御部２４、ＰＨＳシステムＤＢとの通信インタフェース２５、携帯端末との通信インタフェース２６、音声応答機能をもつ音声制御部２７、電話インタフェース２８、および内部バス２９からなる。ＣＰＵ２０は、ＲＯＭ２１に用意された制御プログラムに従って、通信制御部２４および音声制御部２７を制御し、通信インタフェース２５を介してＰＨＳシステムＤＢと、通信インタフェース２６を介して携帯情報端末と、電話インタフェース２８を介して電話機と通信する。ＲＡＭ２２は、プログラムのワークエリアとして利用され、ＰＨＳシステムＤＢあるいは携帯端末所有者からのデータの一時保存に利用される。ファイル装置２３は、セキュリティ管理データレコード、紛失端末からの回収データ、あるいは常駐による保護処理動作に必要な情報等の保存に利用される。

【００４３】図１５は、携帯端末１４の構成を示すブロック図である。本発明を適用する携帯端末１４は、ＣＰＵ３１、ＲＯＭ３２、ＲＡＭ３３Ａおよび３３Ｂ、補助記憶装置３４、表示装置（例えば、液晶ディスプレイ）３５、入力装置３６、電源制御部３７、通信インタフェース３８、通信制御部３９、バス４０、電源制御線４１、通信割り込み制御線４２からなる。ＣＰＵ３１は、バス４０を介して、ＲＯＭ３２、ＲＡＭ３３Ａ、３３Ｂ、補助記憶装置３４、表示装置３５、入力装置３６、通信インタフェース３８との間でデータを送受信する。また、電源制御部３７は、電源制御線４１を介して、上記各要素の電源オン、オフを制御する。通信制御部３９は、本実施例では、ＰＨＳ無線通信を実現するための機能として、例えば、アンテナ、高周波回路、ＰＨＳの通信手順制御および通信内容チェック手段を備え、通常のＰＨＳ通信では、通信インタフェース３８を介してＣＰＵ３１と通信メッセージデータのやり取りを行い、通信割り込み制御信号を発生して、ＣＰＵ３１または電源制御部３７に割り込みをかける。

【００４４】ＲＯＭ３２は、携帯端末としての機能を実現するための各種のソフトウェアと、本発明による端末情報保護を実施するための専用ソフトウェア及び制御情報が格納される。ＲＡＭ３３Ａおよび３３Ｂは、電源でバックアップされており、ＲＡＭ３３Ａは、情報保護を必要としない通常のデータ格納用として、また、ＲＡＭ３３Ｂは、本発明を適用して保護すべき特定ファイルデータの格納用として用いられる。上記携帯端末のＣＰＵは、通信制御部からの割込みを受けると、ＲＯＭ３２に用意された専用ソフトウエアを実行し、上記割込みが端末情報保護命令の受信によるものであれば、ＲＡＭ３３Ｂ内の蓄積情報を保護対象として、前述のデータ回収および保護処理を実行する。

【００４５】上記実施例では、各端末で保護対象となる情報を特定のメモリに蓄積しておき、端末紛失時に上記特定メモリ内の全情報に対して情報保護動作がかかるようにしたが、情報保護はデータファイル名を特定して行

うようにしてもよい。例えば、各携帯端末において、保護対象となる情報を特定のファイル名、または特定の頭文字をもつファイル名で管理しておき、情報保護の登録要求時に、端末所有者が保護対象とすべきファイル名（または頭文字等のファイル識別情報）を指定して、これを上記専用ソフトウエアが記憶しておき、情報保護命令が発生した時、上記特定ファイル名のファイルに対して保護処理を実行するようにしてもよい。

【００４６】また、実施例では、端末所有者が電話機を介してセキュリティコントローラと直接交信し、セキュリティコントローラ側が音声応答機能によって情報保護要求を受付制御するようにしたが、紛失端末の所有者がテキストデータの送受信機能を備えた他の無線端末、またはネットワーク５に接続された他の端末からセキュリティコントローラにアクセスし、端末情報保護に必要な情報をデータメッセージ形式で交信するようにしてもよい。また、紛失端末の所有者が普通の電話機で通報した情報保護要求をセキュリティシステム側で係員が受付け、端末所有者が指定した登録者ＩＤに基づいて係員が専用端末からセキュリティコントローラにアクセスし、所有者の認証に必要なパスワード等のデータを係員端末から入力することによって、情報保護を実行するようにしてもよい。

【００４７】

【発明の効果】以上の説明から明らかなように、本発明によれば、携帯端末の通常の使用時において、ファイルアクセス権限確認のためのパスワード入力等の面倒な操作を強制することなく、携帯端末紛失時に端末情報の保護あるいは情報回収が可能となる。また、情報保護要求時に、無線ネットワークにおける端末位置登録機能を利用すれば、紛失端末の概略的な現在位置を知ることができるため、この位置情報に基づいて紛失端末の回収にも役立つことができる。

【図面の簡単な説明】

【図１】本発明による携帯端末情報保護を実現するネットワークシステムの構成図。

【図２】端末情報保護の登録手順の１実施例を示す図。

【図３】上記端末情報保護の登録時に携帯端末とセキュリティコントローラとの間で通信されるメッセージフォーマットの１実施例を示す図。

【図４】上記端末情報保護の登録時に携帯端末に表示される画面の１実施例を示す図。

【図５】上記端末情報保護の登録時にセキュリティコントローラが実行する制御プログラムの処理手順の１実施例を示すフローチャート。

【図６】端末紛失時に実行されるネットワークで実行される情報保護手順の１例を示すシーケンス図。

【図７】端末紛失時に実行されるネットワークで実行される情報保護手順の他の例を示すシーケンス図。

【図８】端末紛失時に実行されるネットワークで実行される情報保護手順のさらに他の例を示すシーケンス図。

【図９】情報保護時に通信されるメッセージフォーマットの１実施例を示す図。

【図１０】情報保護時にセキュリティコントローラが実行する制御プログラムの１実施例を示すフローチャート。

【図１１】情報保護時にセキュリティコントローラが実行する制御プログラムの他の実施例を示すフローチャート。

【図１２】情報保護時にＰＨＳデータベースシステムが実行する制御プログラムの１実施例を示すフローチャート。

【図１３】情報保護時に携帯端末が実行する制御プログラムの１実施例を示すフローチャート。

【図１４】セキュリティコントローラの構成の１例を示すブロック図。

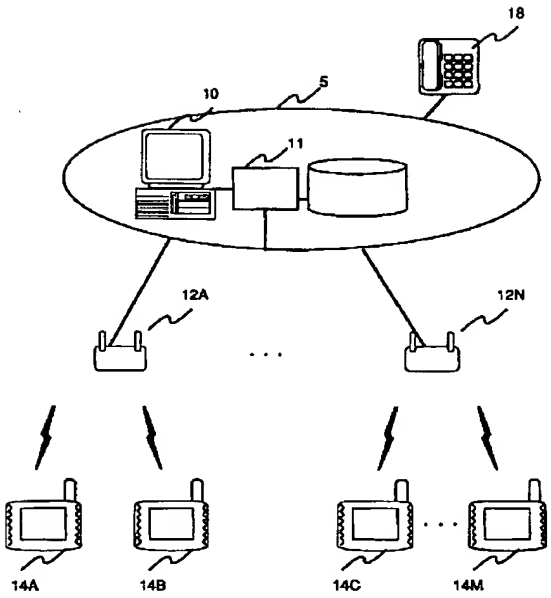
【図１５】携帯端末の構成の１例を示すブロック図。

【符号の説明】

１…無線ネットワークシステム、５…有線網、１０…セキュリティコントローラ、１１…ＰＨＳシステムデータベース、１２…基地局、１４…携帯端末、１８…電話、５１…登録要求、５２…登録情報要求、５３…登録情報、５４…登録情報確認、５５…登録確認応答、５６…登録ＯＫレスポンス、７０…通信メッセージフォーマット、７１…識別ＩＤ、７２…動作ＩＤ、７３…データ量、７４…データ内容、７５…ＣＲＣ、７６…登録要求データ、７７…登録情報データ、７８…登録ＯＫレスポンスデータ、９０…登録開始画面、９１…登録入力画面、９２…所有者確認画面、１２１…保護要求、１２２…認証確認メッセージ、１２３…認証データ、１２４…要求確認メッセージ、１２５…要求送付、１２６…終了通知、１２７…携帯端末検索要求、１２８…携帯端末検索レスポンス、１２９…情報保護命令、１３０…保護終了報告及び保護データ、１５１…常駐確認メッセージ、１５２…常駐レスポンス、１５３…連絡先確認メッセージ、１５４…連絡先レスポンス、１５５…終了メッセージ、３０１…携帯端末検索データ、３０２…携帯端末検索レスポンスデータ、３０３…情報保護命令データ、３０４…保護データ。

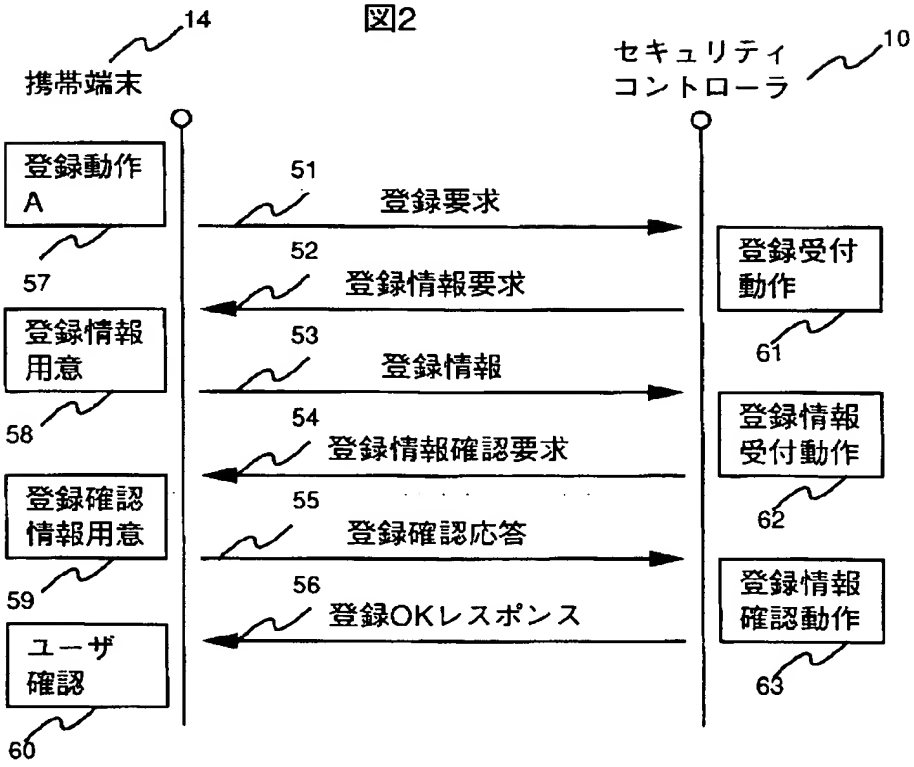
【図１】

図1


1
18
10
5
11
12A
12N
14A
14B
14C
14M

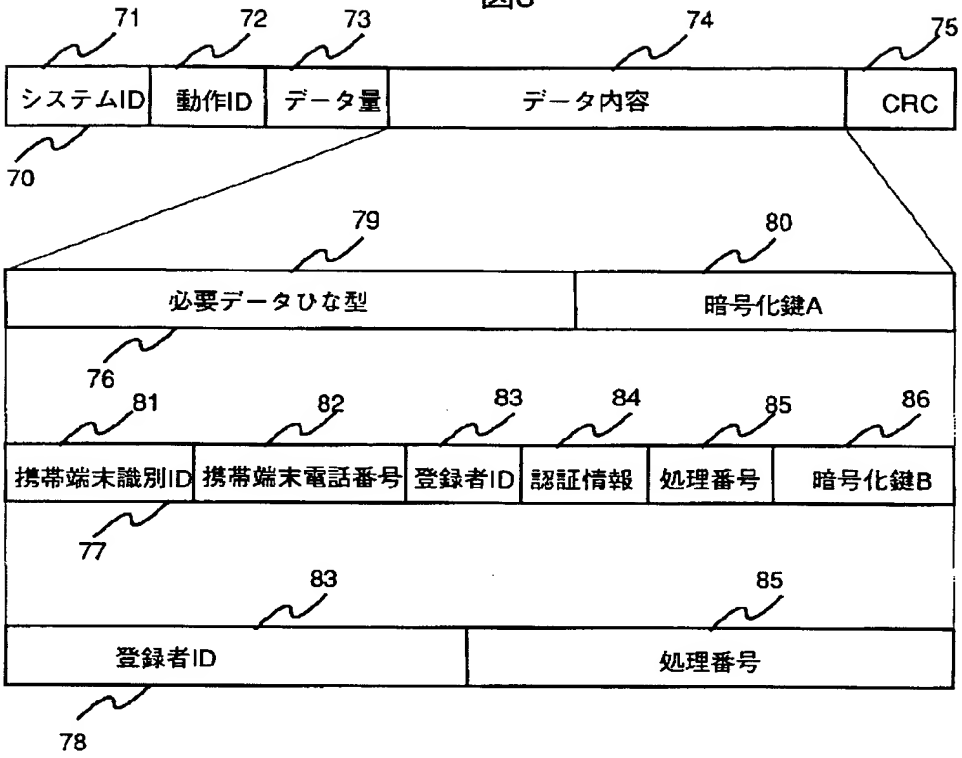
【図２】

図2


14
携帯端末
セキュリティ
コントローラ
10
登録動作
A
57
登録情報
用意
58
登録確認
情報用意
59
ユーザ
確認
60
51
登録要求
52
登録情報要求
53
登録情報
54
登録情報確認要求
55
登録確認応答
56
登録OKレスポンス
登録受付
動作
61
登録情報
受付動作
62
登録情報
確認動作
63

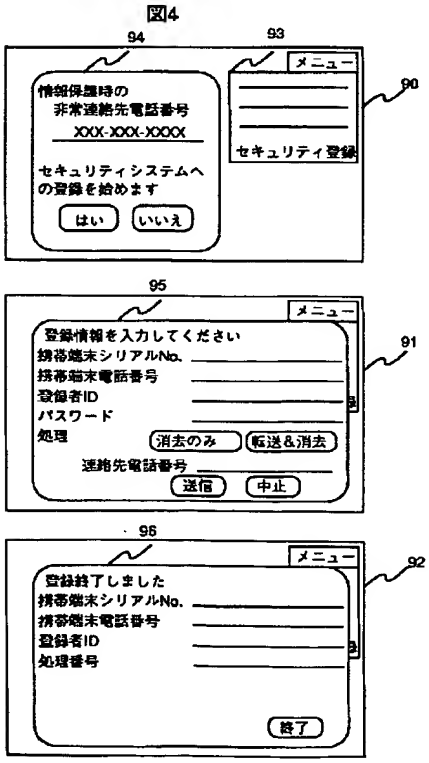
【図３】

図3



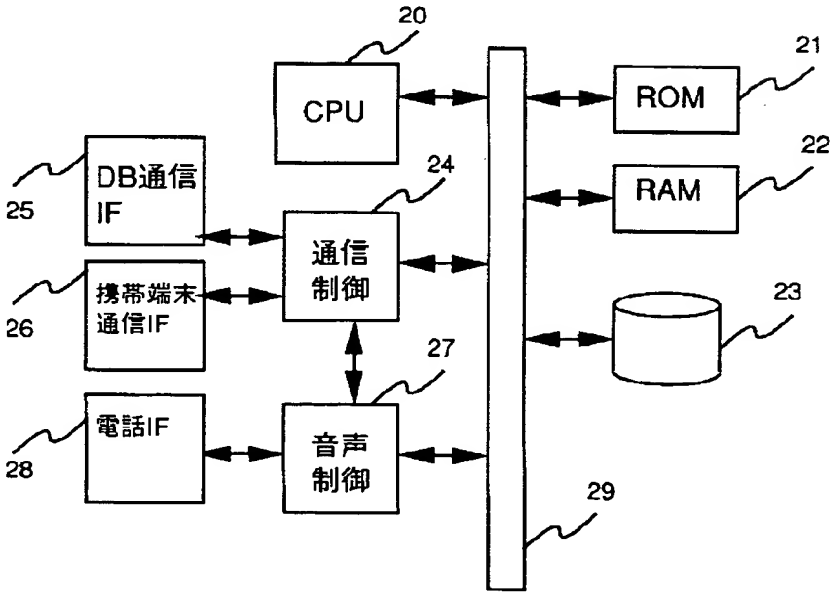
【図４】

図4



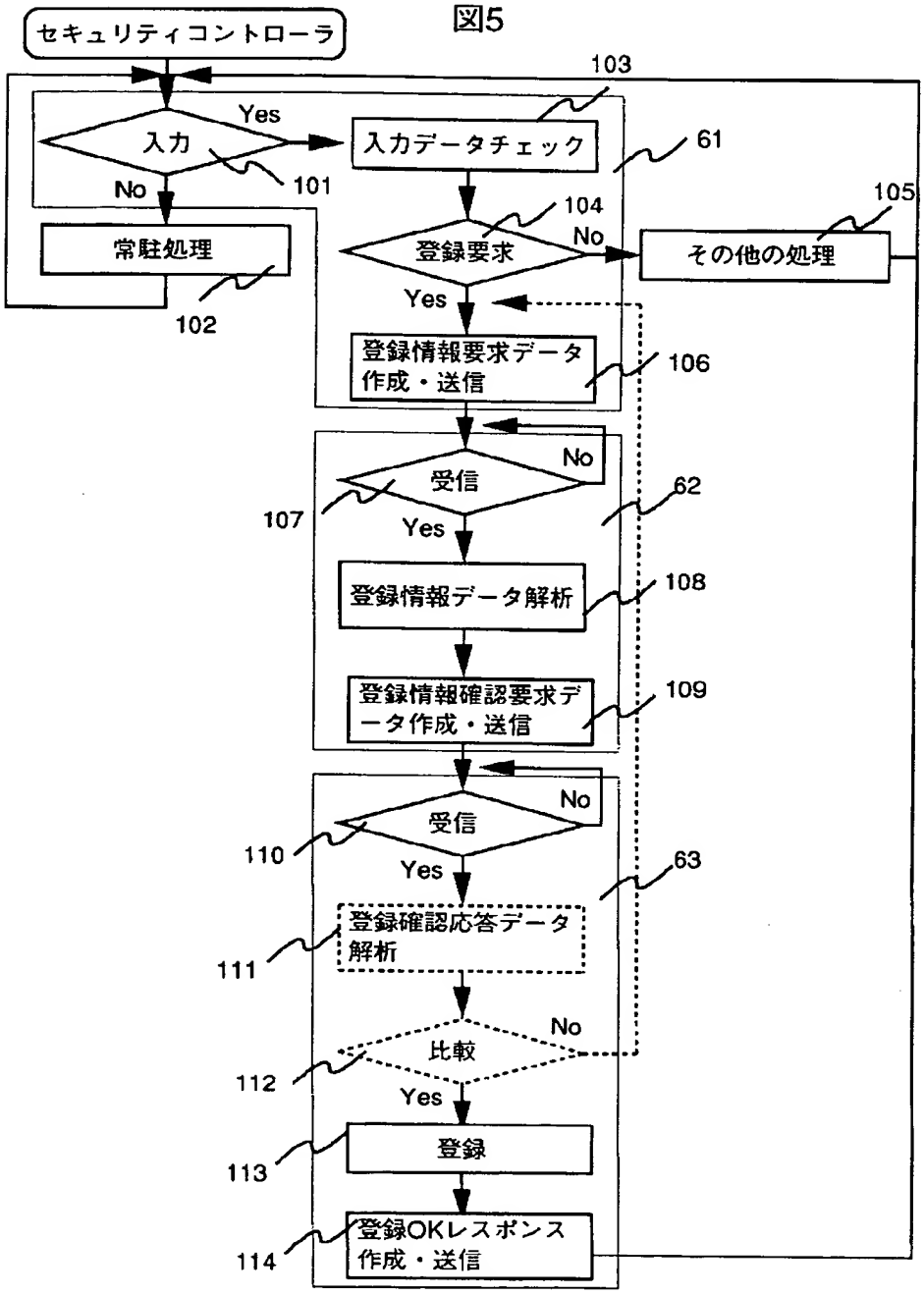
【図１４】

図14



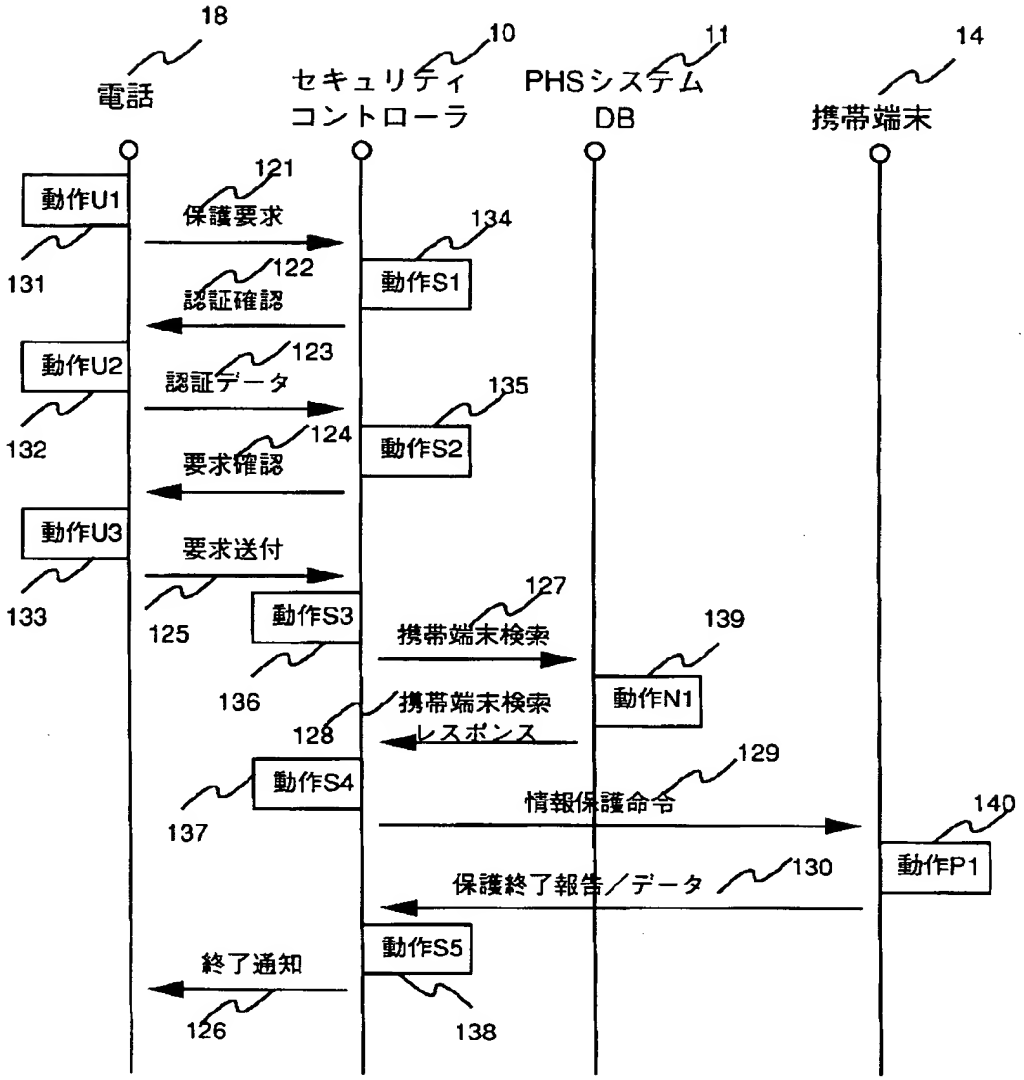
【図５】

図5


セキュリティコントローラ
103
Yes
入力
入力データチェック
61
101
No
105
常駐処理
104
登録要求
No
その他の処理
Yes
102
登録情報要求データ作成・送信
106
No
受信
62
107
Yes
登録情報データ解析
108
登録情報確認要求データ作成・送信
109
No
受信
110
Yes
63
登録確認応答データ解析
111
No
比較
112
Yes
登録
113
登録OKレスポンス作成・送信
114

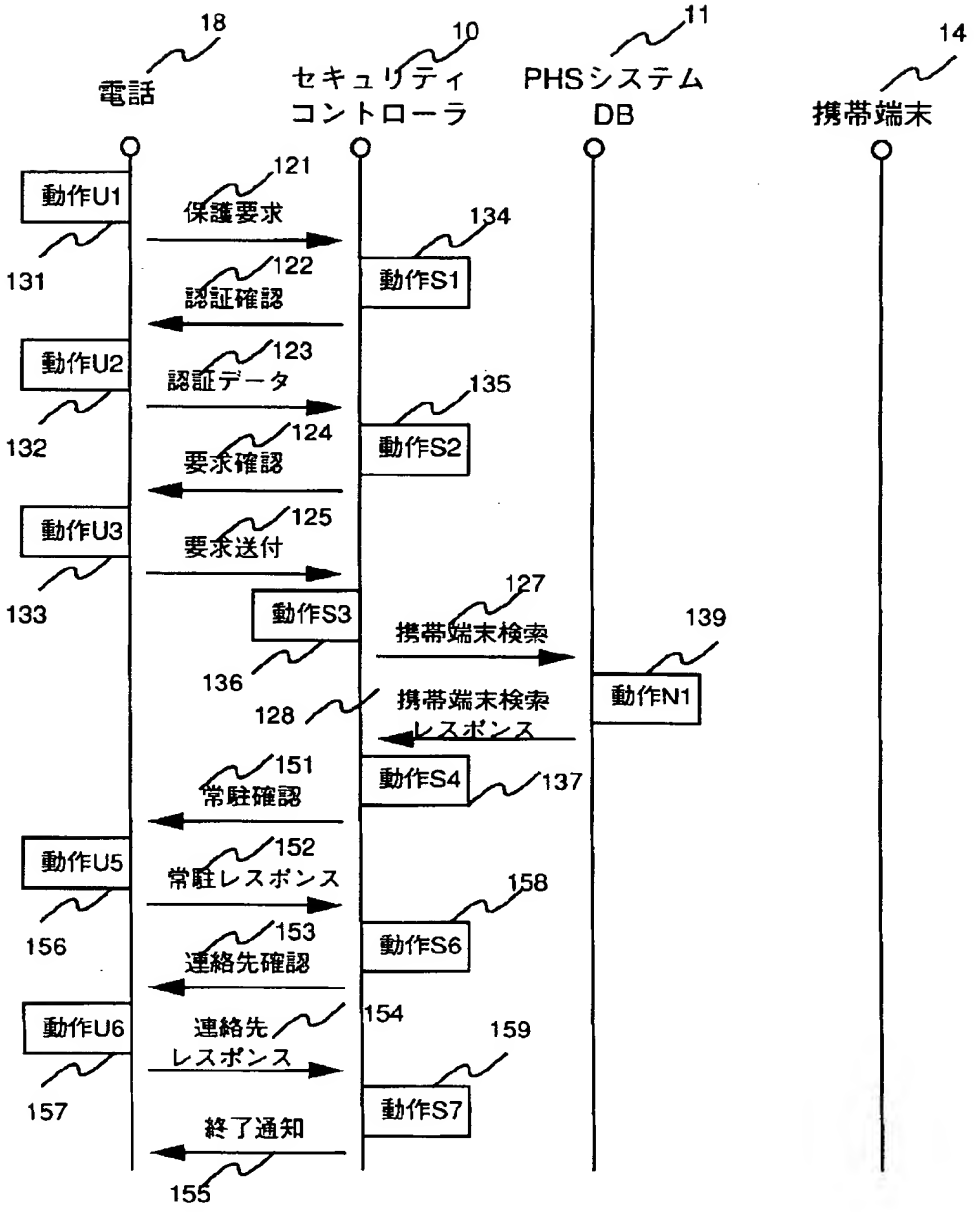
【図６】

図6


18
電話
10
セキュリティ
コントローラ
11
PHSシステム
DB
14
携帯端末
動作U1
121
保護要求
131
134
動作S1
122
認証確認
動作U2
123
認証データ
132
135
動作S2
124
要求確認
動作U3
要求送付
133
125
動作S3
127
携帯端末検索
139
136
動作N1
128
携帯端末検索
レスポンス
129
動作S4
情報保護命令
140
137
動作P1
保護終了報告／データ
130
動作S5
終了通知
126
138

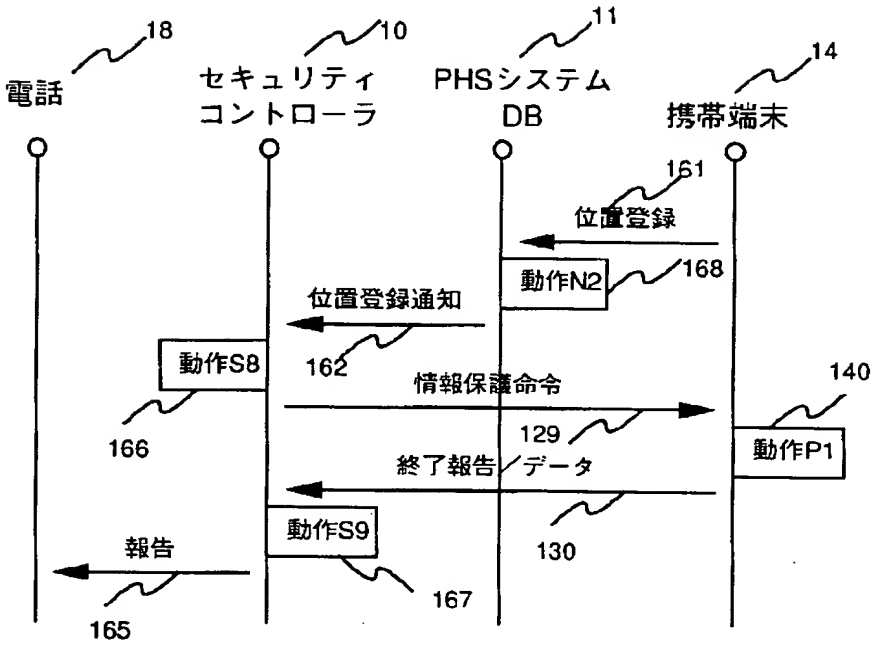
【図７】

図7


18
電話
10
セキュリティ
コントローラ
11
PHSシステム
DB
14
携帯端末
動作U1
131
121
保護要求
134
動作S1
122
認証確認
動作U2
132
123
認証データ
135
動作S2
124
要求確認
動作U3
133
125
要求送付
127
動作S3
携帯端末検索
139
136
動作N1
128
携帯端末検索
レスポンス
151
常駐確認
動作S4
137
動作U5
156
152
常駐レスポンス
158
動作S6
153
連絡先確認
動作U6
157
154
連絡先
レスポンス
159
動作S7
終了通知
155

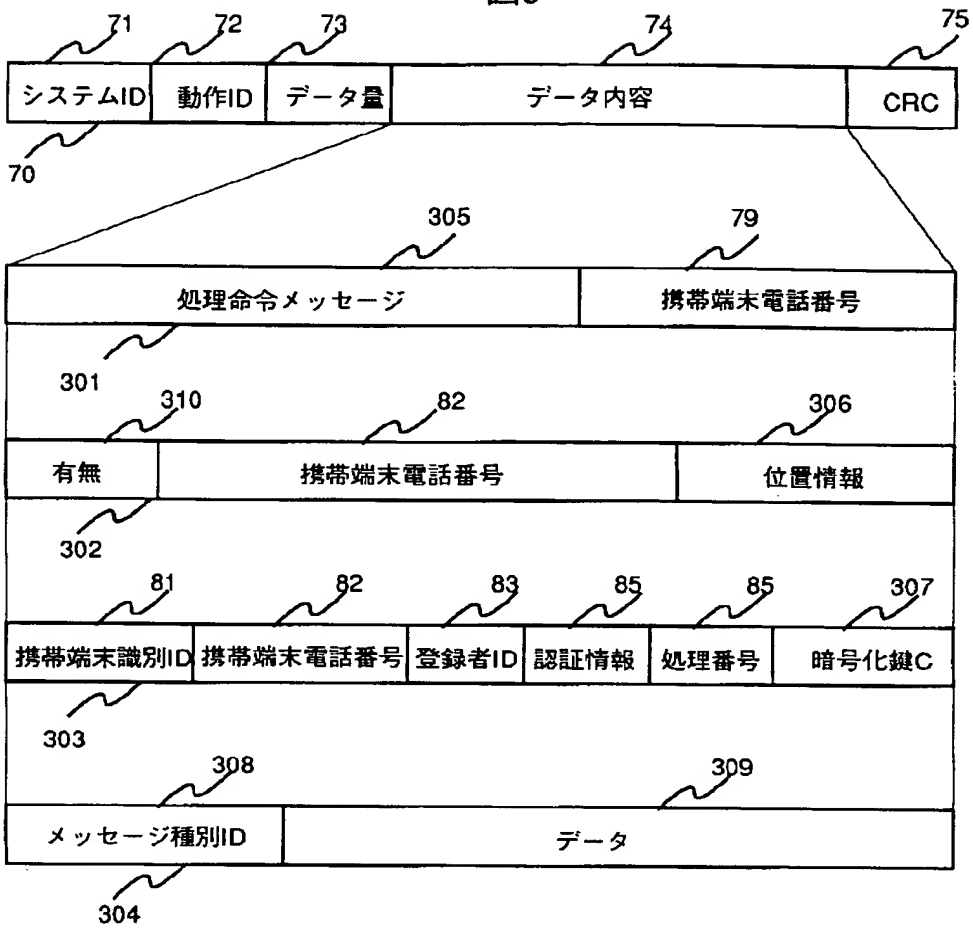
【図８】

図8


18
電話
10
セキュリティ
コントローラ
11
PHSシステム
DB
14
携帯端末
161
位置登録
動作N2
168
位置登録通知
162
動作S8
166
情報保護命令
140
129
データ
動作P1
終了報告
130
動作S9
167
報告
165

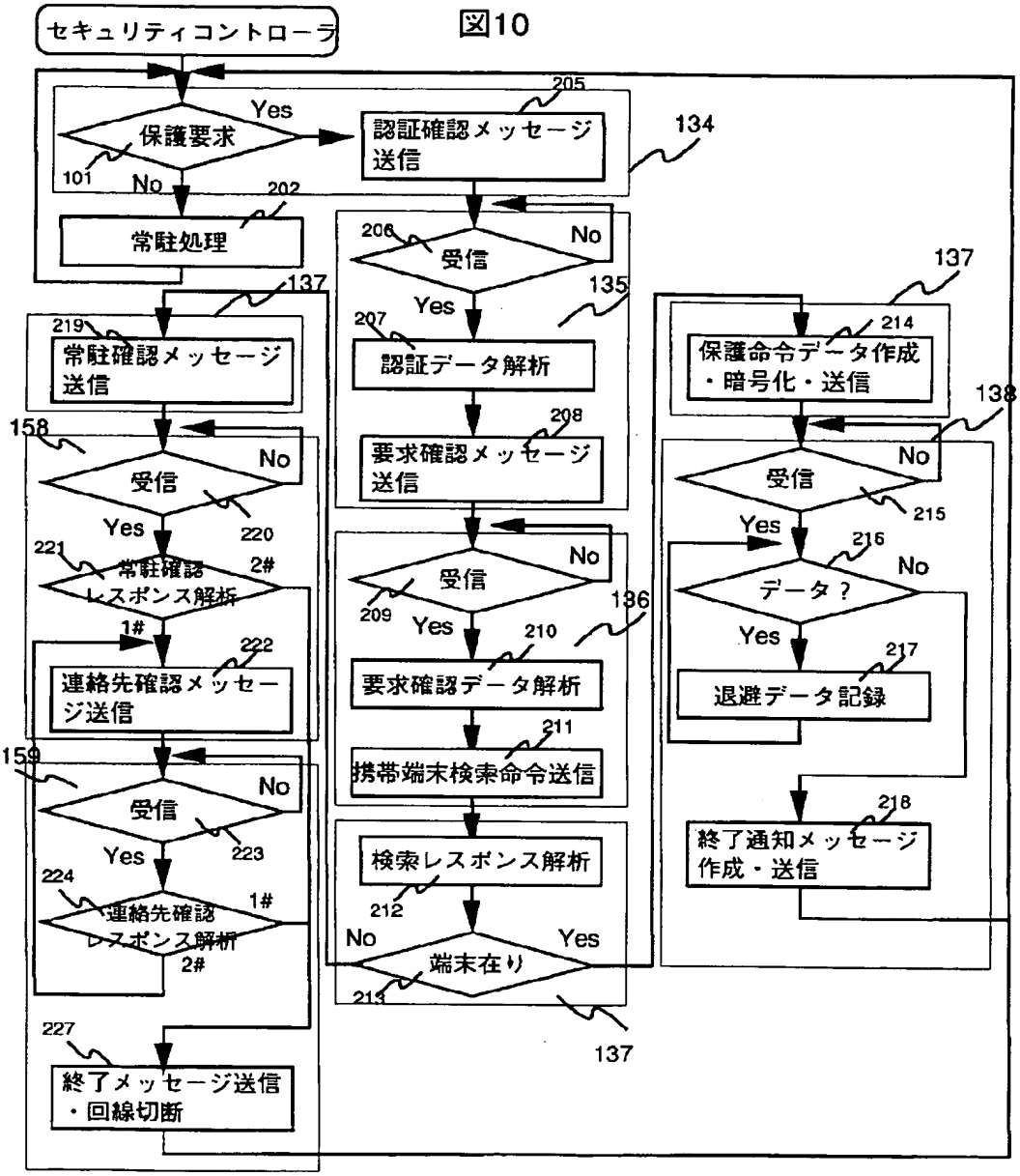
【図９】

図9


71
72
73
74
75
システムID
動作ID
データ量
データ内容
CRC
70
305
79
処理命令メッセージ
携帯端末電話番号
301
310
82
306
有無
携帯端末電話番号
位置情報
302
81
82
83
85
85
307
携帯端末識別ID
携帯端末電話番号
登録者ID
認証情報
処理番号
暗号化鍵C
303
308
309
メッセージ種別ID
データ
304

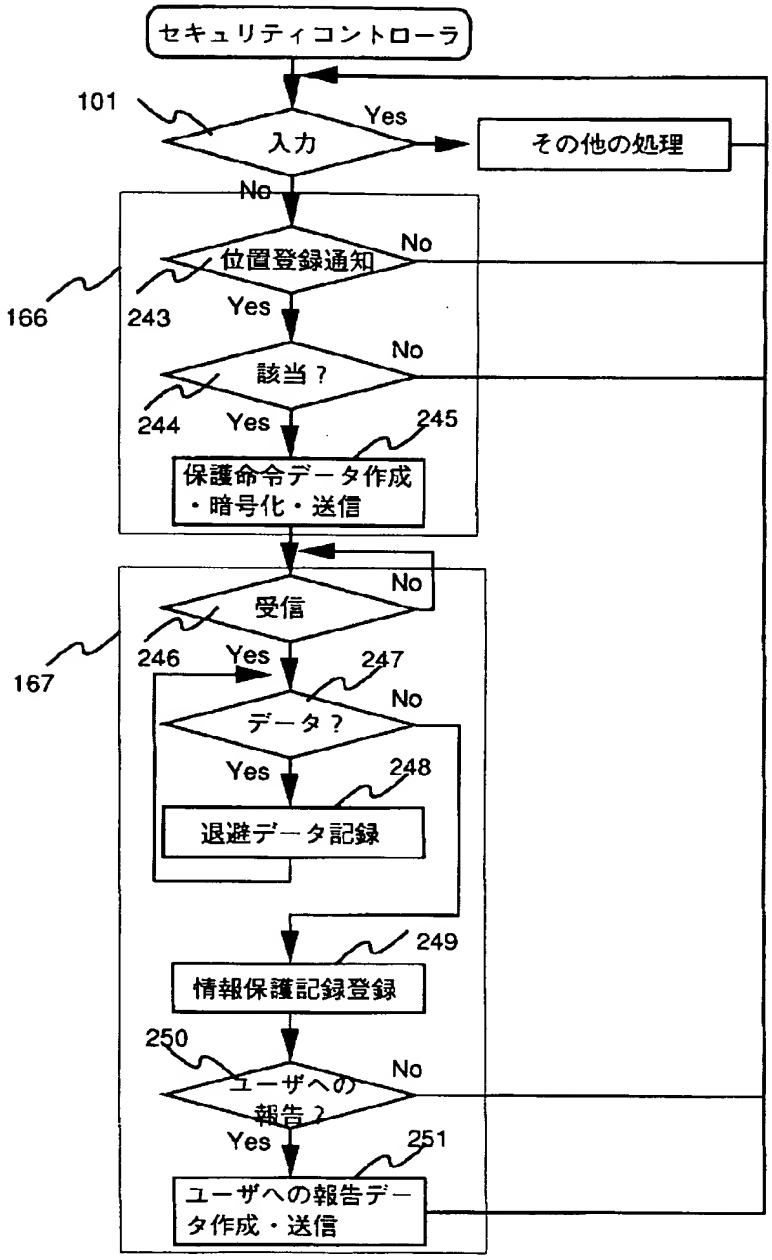
【図１０】

図10


セキュリティコントローラ
保護要求
Yes
No
101
認証確認メッセージ送信
205
134
常駐処理
202
受信
206
No
Yes
135
認証データ解析
207
要求確認メッセージ送信
208
137
常駐確認メッセージ送信
219
158
受信
No
Yes
220
常駐確認レスポンス解析
221
2#
1#
連絡先確認メッセージ送信
222
159
受信
No
Yes
223
連絡先確認レスポンス解析
224
1#
2#
227
終了メッセージ送信・回線切断
受信
No
209
Yes
要求確認データ解析
210
136
携帯端末検索命令送信
211
検索レスポンス解析
212
No
Yes
端末在り
213
137
137
保護命令データ作成・暗号化・送信
214
138
受信
No
215
Yes
データ？
216
No
Yes
退避データ記録
217
終了通知メッセージ作成・送信
218

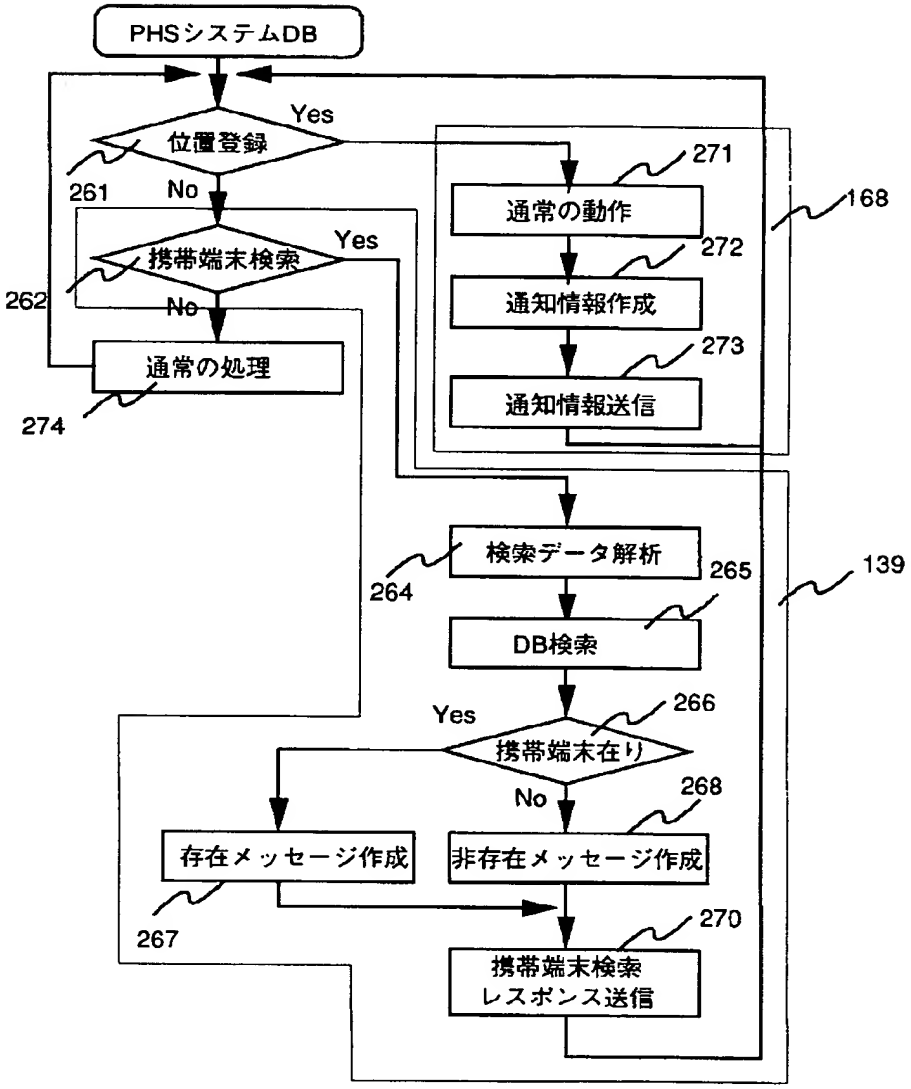
【図１１】

図11


セキュリティコントローラ
101
入力
Yes
その他の処理
No
位置登録通知
No
166
243
Yes
該当？
No
244
Yes
245
保護命令データ作成
・暗号化・送信
No
受信
246
Yes
247
167
データ？
No
Yes
248
退避データ記録
249
情報保護記録登録
250
ユーザへの
報告？
No
Yes
251
ユーザへの報告デー
タ作成・送信

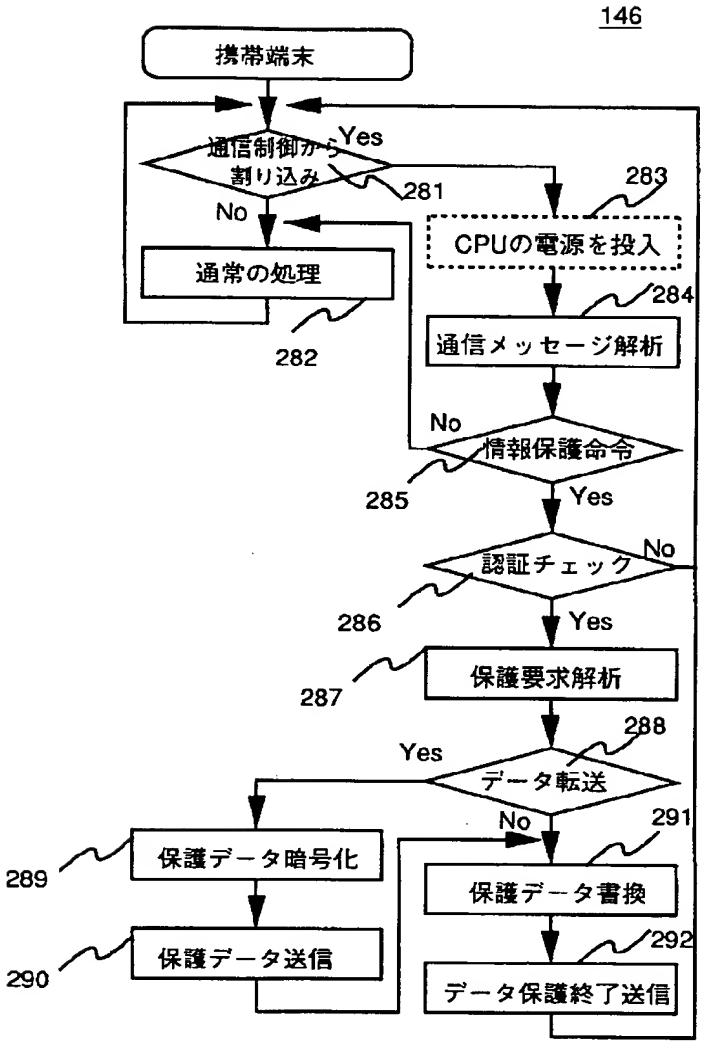
【図１２】

図12


PHSシステムDB
位置登録
Yes
No
261
携帯端末検索
Yes
No
262
通常の処理
274
271
通常の動作
272
通知情報作成
273
通知情報送信
168
検索データ解析
264
265
DB検索
139
Yes
266
携帯端末在り
No
268
存在メッセージ作成
非存在メッセージ作成
267
270
携帯端末検索
レスポンス送信

【図１３】

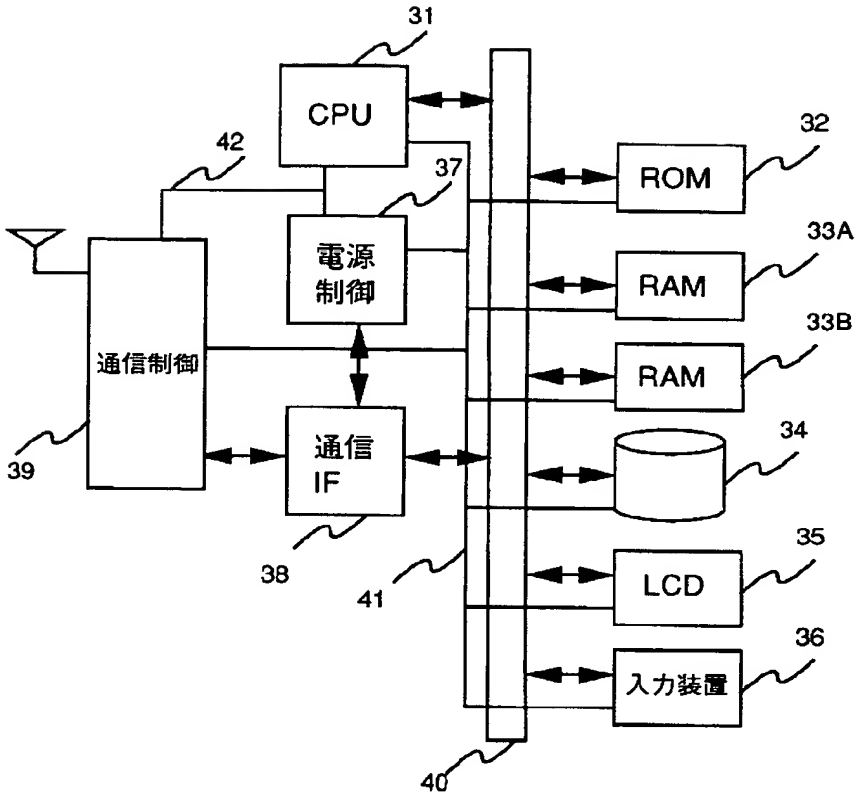
図13


146
携帯端末
通信制御から割り込み
Yes
281
No
283
CPUの電源を投入
通常の処理
282
284
通信メッセージ解析
No
情報保護命令
285
Yes
No
認証チェック
286
Yes
287
保護要求解析
288
Yes
データ転送
No
291
289
保護データ暗号化
保護データ書換
290
保護データ送信
292
データ保護終了送信

【図１５】

図15

14



フロントページの続き

(51)Int.Cl.⁶	識別記号	庁内整理番号	FI		技術表示箇所
Ｈ０４Ｍ　11/00	３０２		Ｈ０４Ｌ　9/00	６７３Ａ	
			Ｈ０４Ｑ　7/04	Ｄ	

Japanese Patent Application, Laid-Open Publication No. H9-215057

INT. CL.[6]:	H04Q	7/38
	G06F	1/00
	G09C	1/00
	H04L	9/32
	H04M	3/42
		11/00

PUBLICATION DATE: August 15, 1997

TITLE Portable Terminal and Portable Terminal Information Protecting Method

APPLICATION NO. H8-16402

FILING DATE February 1, 1996

APPLICANT(S) KK HITACHI SEISAKUSHO

INVENTOR(S) Muneaki YAMAGUCHI

ABSTRACT

PROBLEM To offer an information protecting system and portable terminal which simplifies the use of the terminal during normal use, and enabling protection and removal of personal information remaining in the terminal when the terminal is lost.

SOLUTION Security control data of a portable terminal 14 is registered in a security controller 10 connected to a radio network in accordance with a registered request for information protection issued from the terminal. When the terminal is lost, if the owner of the portable terminal requests information protection of the security controller, an information protection instruction is sent through the radio network to the portable terminal, and important information in the terminal is removed and recovered to the security controller and nullified by means of an exclusive program inside the portable terminal.

EFFECTS Important information can be removed even if a portable terminal is lost, thereby prohibiting misuse.

CLAIMS

1. A portable terminal device comprising radio communication means, output means, input means, memory means for storing user data, and data processing means for writing and reading user data with respect to said memory means, outputting information to said output means and exchanging information with other devices through said radio communication means in response to user operation inputs from said input means; characterized by comprising:

means for storing verification information for verifying information protection requesters with respect to data stored in said memory means; and

information protecting software containing a predetermined data processing procedure for checking the validity of an information protection request from the correspondence relationship between verification information included in a information protection instruction message received by said radio communication means and verification information prestored in said memory means, and if confirmed to be valid, nullifying specific user data stored in said memory means;

said data processing means running said information protecting software in response to a notice from said radio communication means to nullify said specific user data and prohibit use by other parties.

2. A portable terminal device as recited in claim 1, characterized in that said memory means comprises a general information region and a protected information region; and

said data processing means nullifies the user data stored in said protected information region by running said information protecting software.

3. A portable terminal device as recited in claim 1, characterized in that said information protecting software prepossesses file identification information for the user data to be protected which is stored in said memory means, and

said data processing means nullifies the user data stored in said protected information region by running said information protecting software.

4. A portable terminal device ac recited in any one of claims 1-3, characterized in that said information protecting software includes a procedure for sending said user data to the transmission source of said information protection instruction message prior to nullifying the user data; and

said data processing means, by running said information protecting software, collects specific user data in another device, then nullifies it.

5. A portable terminal device as recited in any one of claims 1-3, characterized in that said information protecting software includes a procedure for selectively sending said user data to the transmission source device of said information protection instruction message in response to a processing category code included in said information protection instruction message; and

said data processing means, by running said information protecting software, performs a removal operation of the user data selectively to recover to another device, then nullifies it.

6. A portable terminal device as recited in claim 4 or 5, characterized in that said information protecting software nullifies said user data by deleting the data.

7. A portable terminal device as recited in claim 4 or 5, characterized in that said information protecting software nullifies said user data by means of data conversion.

8. A portable terminal device as recited in any one of claims 1-7, characterized by comprising power supply control means for automatically turning on the power supply to said data processing means and said memory means in response to an interruption signal outputted from said radio communicating means upon receiving said information protection request message.

9. A portable terminal information protecting method characterized by comprising:

a step of registering in a security control device security control data necessary for protection of user information held by the portable terminal;

a step of an owner of a portable terminal requesting said security device to perform information protection with respect to a lost portable terminal;

a step of the security control device which has received said information protection request generating an information protecting instruction message based on pre-registered security control data, and sending it through the radio network to said lost portable terminal; and

a step of the portable terminal which has received said information protection message processing predetermined user information held in said terminal to prohibit use by others.

10. A portable terminal information protecting method as recited in claim 9, characterized in that said security control device checks whether or not communications by the radio network are possible for the portable terminal requesting information protection; confirming that it is in a communicable state, and sending said information protection instruction message.

11. A portable terminal information protecting method as recited in claim 10, characterized in that said security control device checks whether or not communications by the radio network are possible for the portable terminal requesting information protection; and if in an incommunicable state, repeats the check of whether radio communications with said portable terminal are possible with a predetermined repetition pattern.

12. A portable terminal information protecting method as recited in claim 9, characterized in that said security control device inquires of a mobile terminal data management device connected to the radio

network as to the state of the portable terminal requesting information protection;

said mobile terminal data management device receiving said inquiry notifies said security control device as to the presence of a position registration of said portable terminal, and if the current position is unregistered, records that a state inquiry has been received for said portable terminal, and notifies said security control device when said portable terminal's position is registered; and

said security management device sends said information protection instruction message in response to the notification from said mobile terminal data management device.

13. A portable terminal information protecting method as recited in any one of claims 9-12, characterized in that:

security management data registered in said security control device includes address information of the portable terminal, registrant identification information and registrant verification information; when requesting said information protection, the requester gives his own identification information and verification information; and said security control device checks the validity of said requester based on the given verification information and the information already registered as security management data, and if confirmed to be valid, generates and sends said information protection instruction message.

14. A portable terminal information protecting method as recited in claim 13, characterized in that the information protection instruction message sent from said security control device includes said verification information; and

the portable terminal which has received said information protection instruction message checks the validity of said received message based on verification information extracted from said received message and verification preset inside said portable terminal, and if validity is confirmed, executes data processing for prohibiting use of said predetermined user information by others.

15. A portable terminal information protecting method as recited in any one of claims 9-14, characterized in that the portable terminal which has received said information protection instruction message performs data processing of predesignated user information in a predetermined memory area to prohibit use by others.

16. A portable terminal information protecting method as recited in any one of claims 9-14, characterized in that the security management data registered in said security control device includes file identification information for specifying information to be protected, and said security control device sets said file identification information in said information protection instruction message; and

the portable terminal which has received said information protection message performs data processing of the user information specified by the file identification information in the received message

to prohibit use by others.

17. A portable terminal information protecting method as recited in any one of claims 9-16, characterized in that the portable terminal which has received said information protection instruction message performs data processing to prohibit use by others after sending said predetermined user information which is to be protected to said security control device.

18. A portable terminal information protecting method as recited in claim 17, characterized in that the portable terminal which has received said information protection instruction message sends said predetermined user information to be protected to said security control device in a state of encryption by means of an encryption key designated in said message.

19. A portable terminal information protecting method as recited in any one of claims 9-18, characterized in that the portable terminal which has received said information protection instruction message prohibits use by others by deleting said predetermined user information to be protected.

20. A portable terminal information protecting method as recited in any one of claims 9-18, characterized in that the portable terminal which has received said information protection instruction message prohibits use by others by performing data conversion on said predetermined user information to be protected.

21. A portable terminal information protecting method as recited in any one of claims 9-20 characterized in that the registration of said security management data to said security control device is performed from the portable terminal device to be protected through a radio network.

22. A portable terminal information protecting method as recited in any one of claims 9-21, characterized in that the information protection request to said security control device is performed using a telephone.

23. A portable terminal information protecting system characterized by comprising a portable terminal, a radio network, and a security control device connected to said radio network;

said security control device comprising memory means for storing security management data relating to portable terminals, and message generating-sending means for generating a data protection instruction message based on said security management data and sending this through said radio network to said portable terminal in response to a data protection request from the owner of a portable terminal which has been lost; and

a portable terminal which has registered security management data with said security control device comprising radio communication means for communicating with said radio network, data processing means and specialized software to be executed by said data processing means in response to a

data protection instruction message received by said radio communication means.

24. A portable terminal information protecting system as recited in claim 23, characterized in that said security control device comprises determining means for determining, upon receiving a data protection request from the owner of said portable terminal, whether or not to accept said protection request based on personal identification information given by said owner and personal verification information preregistered as said security management data, and generating and sending said data protection instruction message for data protection requests determined to be acceptable.

25. A portable terminal information protecting system as recited in claim 24, characterized in that:

the message generating-sending means of said security control device sends said data protection instruction message with personal verification information preregistered as said security management data included in said message;

said portable terminal comprises determining means for determining whether or not it is possible to respond to said data protection instruction message based on personal verification information included in the received data protection instruction message and personal verification information prestored in said portable terminal; and

performs data processing of said specific data in response to a data protection instruction message for which said determining means has determined that response is possible.

26. A portable terminal information protecting system as recited in any one of claims 23-25, characterized in that said portable terminal radio communication means comprises power supply control means for discriminating said data protection instruction message and automatically turning on the power supply to said data processing means.

27. A portable terminal information protecting system as recited in any one of claims 23-26, characterized in that the specialized software of said portable terminal, after transfer of said specified data to said security control device, invalidates data with respect to others by means of data deletion or data encryption.

28. A portable terminal information protecting system as recited in claim 27, characterized in that said portable terminal comprises means for encrypting data transferred to said security control device.

DETAILED DESCRIPTION OF THE INVENTION

Technical Field

The present invention relates to a portable terminal and portable terminal information protecting method,

more specifically to a mobile terminal comprising a microprocessor, memory mean sand radio communication means, and a method for protecting user information stored in the memory.

Conventional Art

Due to improvements in electronics technology such as semiconductor memories and microprocessors, portable terminal devices known as electronic notebooks, personal digital assistants (PDA's) and new portable information tools are being put into practice in addition to notebook-type personal computers. In particular, portable terminal devices which have become more compact and lightweight are able to be put into the pocket of one's jacket and readily carried, and their manner of use is also diversifying with data input/output operations possible while moving, and exchange of data with the office-side information processing system from a remote location using communication capabilities.

Thus, since these portable terminal devices can be carried outside the office or put inside a bag or a pocket to be carried, the chances of loss or misplacement due to carelessness or falling into someone else's hands against the owner's intentions also grow, thus increasing the risk of information stored in the terminal device being seen or abused by a third party. Conventionally, as a method for protecting information requiring a high level of security, a password is appended to an information file whose access is to be restricted, such that when a user attempts to look at this information file, the system prompts the input of the password, allowing access only when the inputted password matches a preregistered valid password.

Problems to be Solved by the Invention

Portable terminals are primarily used as the possessions of individuals, and are not assumed to be shared by an unspecified plurality of users such as individual terminals equipped inside offices, nor lent to others. For this reason, it is rare for the owner of a portable terminal to pay any heed to the protection of user information inside a portable terminal while the terminal is under his own control. Additionally, the owners of portable terminals desire that the information stored in the portable terminals be readily at hand as their own possessions, so that even if there is information which is not for others' eyes, privacy protection measures such as passwords mentioned above, which are procedurally troublesome, are often not taken so that the terminals can be used in an operating environment enabling continuous and quick access to the required information. Owners of portable terminals usually become aware of the need to prevent viewing and use of information stored in the terminal by others only after they lose their terminals.

The purpose of the present invention is to offer a portable terminal device, a terminal information protecting method and terminal information protecting system capable of prohibiting abuse of information which is important to the owner which remains inside the terminal after the terminal has been lost. Another purpose of the present invention is to offer a portable terminal device, terminal information protecting method and terminal information protecting system enabling user information important to the owner which remains inside the terminal after the terminal has been lost to be recovered into the hands of the owner. Another purpose of the present invention is to offer a portable terminal device, a terminal information protecting method and terminal information protecting system wherein information stored in a terminal can always be readily accessed, but capable of protecting user information important to the owner which remains inside the terminal after the terminal has been lost.

Means for Solving the Problems

In order to achieve the above-described purposes, the portable terminal information protecting method and protecting system of the present invention are characterized by registering in a security control device security control data necessary for protection of user information held by the portable terminal; an owner of a portable terminal requesting the security device to perform information protection with respect to a lost portable terminal; the security control device which has received the information protection request

generating an information protecting instruction message based on pre-registered security control data, and sending it through the radio network to the lost portable terminal; and the portable terminal which has received the information protection message processing predetermined user information held in the terminal to prohibit use by others.

According to an embodiment of the present invention, the above-described security control device checks whether or not communications by the radio network are possible for the portable terminal requesting information protection; confirming that it is in a communicable state, and sending the information protection instruction message. Prior to sending the information protection instruction message, the security control device inquires of a mobile terminal data management device connected to the radio network as to the state of the portable terminal requesting information protection; the mobile terminal data management device receiving the inquiry notifies the security control device as to the presence of a position registration of the portable terminal, and if the current position is unregistered, records that a state inquiry has been received for the portable terminal, and notifies the security control device when the portable terminal's position is registered; and the security management device sends the information protection instruction message in response to the notification from the mobile terminal data management device.

In the present invention, the security management data includes portable terminal address information (an address or telephone number on the radio network), registrant identification information and registrant verification information. By preregistering this type of management data in the security control device, at the time of a request for information protection, it is possible to have a requester (owner of a lost portable terminal) give his own identification information and verification information, to enable the security control device to collate the given information with the information which has previously been registered as security management data to check the validity of the requester, to enable the information protection instruction message to be generated and sent only when validity has been confirmed. Additionally, it is possible to set the verification information in the information protection instruction message sent to the portable terminal, and to have the portable terminal which received the information protection instruction message check the validity of the received message based on the verification information extracted from the received message and the verification information preset in the portable terminal, so as to perform data processing for protection of the information only in the case where validity has been confirmed.

The portable terminal according to the present invention is a portable terminal device comprising radio communication means, output means, input means, memory means for storing user data, and data processing means for writing and reading user data with respect to the memory means, outputting information to the output means and exchanging information with other devices through the radio communication means in response to user operation inputs from the input means; characterized by comprising: means for storing verification information for verifying information protection requesters with respect to data stored in the memory means; and information protecting software containing a predetermined data processing procedure for checking the validity of an information protection request from the correspondence relationship between verification information included in a information protection instruction message received by the radio communication means and verification information prestored in the memory means, and if confirmed to be valid, nullifying specific user data stored in the memory means; the data processing means running the information protecting software in response to a notice from the radio communication means to nullify the specific user data and prohibit use by other parties.

In order to specify the user data to be protected, the portable terminal of the present invention, for example, divides the memory means into a general information area and a protected information area, such as to nullify the user data stored in the protected information area for information protection. As forms for protection of the user data, it is possible to transfer the user data to another device, such as the transmission source of the information protection request message, enabling it to be recovered into the hands of the terminal owner later. In this case, the user data may be transferred in an encrypted state.

Embodiments of the Invention

Fig. 1 shows the overall structure of a system for achieving a portable terminal information protecting method according to the present invention using a radio network. In the drawing, reference number 1 denotes a radio network composed of a plurality of radio base stations 12 (12A-12N) interconnected through a wire network 5 and a database system 11 storing mobile terminal control data, and 10 denotes a security controller (security server) connected to the radio network. 14 (14A-14M) denotes a mobile terminal using the radio network, and the portable information terminal (hereinafter referred to simply as a portable terminal) to which the present invention is directed aside from a normal mobile telephone is one type of such mobile terminals. In the following embodiment, a case of applying a PHS (Personal Handyphone System) as a radio network 1 shall be explained. A stationary terminal 18 and other public telephone communication networks are connected to the wire network 5 through a switching system which is not shown. However, it is possible to use another system enabling communication of messages containing computer commands and data between the portable terminal and security controller in the above-described radio network.

The above-described database system (PHS system DB) 11 manages position information and verification information of the mobile terminals (PHS telephones and portable terminals with internal PHS functions) as mobile terminal control data, and in the present embodiment, the security controller 10 is connected to the database system. The security controller 10 registers security management data required for information protection of the portable terminal 14 in response to a security registration request from the owner of a portable terminal 14, and upon receiving a portable terminal information protection request from the user through a communication device of a telephone 18 or the like, performs verification of the user and identification of the portable terminal based on the pre-registered security management data, and through the radio network system, obtains the current position information of a target terminal and performs a protection operation on the information as shall be described below. The position information of the portable terminal 14 is obtained by accessing the PHS system DB 11, and information protection is achieved by sending an information protection instruction to the portable terminal 14, and performing the information protection program contained in the portable terminal.

Fig. 2 shows the procedure for registration of information protection to the security controller 10 by means of the owner of a portable terminal. When a registration operation 57 is performed at the portable terminal 14, it is connected to the security controller 10 and a registration request 51 is sent to the security controller 10. In response to the registration request 51, the security controller 10 runs a registration acceptance operation 61 and sends a registration information request 52 to the portable terminal 14 making the request. The portable terminal 14 inputs information necessary for information protection of the owner in response to the registration information request, and sends this as registration information 53 to the security controller 10. The security controller 10 analyzes the above-described registration information 53, then sends a registration information confirmation request 54 to the portable terminal 4. Once the owner confirms that there are no errors in the registration content, the registration confirmation response 55 is sent from the portable terminal 14 to the security controller 10. When the security controller 10 receives the registration confirmation response, it performs a registration information confirmation operation 63, registers the registration information 53 in the registration data table, and sends a registration OK response 56 to the portable terminal 14 to end the registration procedure. Similarly, at the portable terminal side, the registration OK response 56 is received, and the user confirms this to end the registration process.

Fig. 3 shows a message format 70 for portable terminal information protection transmitted between the portable terminal and the security controller. The message 70 is composed of five fields, that is, the system ID 71, the operation ID 72, the data quantity 73, the data content 74 and the CRC (cyclic redundancy check) 75. The system ID 71 is set with a code indicating that this message is for portable terminal information protection. The operation ID 72 shows the type of message, having set therein an identifier for identifying the registration request 51, registration information request 52 and the like.

The data quantity 73 indicates the amount of data in the subsequent data content field 74 in units of bytes, and the CRC 75 is used for a data error check from the operation ID field 72 to the data content field 74.

The data content 74 of the registration information request message 52 sent from the security controller 10 to the portable terminal in response to the registration request 51 contains a required data template 79 and an encryption key A:80 as shown in the data format 76. The required data template 79 is data for displaying to the owner of a portable terminal the information categories required as registered information 53, and is composed of a character string representing the information categories to be inputted and the byte length thereof. The encryption key A:80 is, for example, a public encryption key in a public key encryption format, wherein the portable terminal 14 sends the registered information 53 to the security controller in a state of encryption using the above encryption key A.

The data content 74 of the registered information message 53, as shown in the data format 77, contains a portable terminal identifying ID 81, a portable terminal telephone number 82, a registrant ID 83, verification information 84, processing number 85 and encryption key B:86. The portable terminal identifying ID 81 is a serial number of the portable terminal, which is used when the security controller is communicating with the portable terminal to determine whether it is communicating with the correct portable terminal. The portable terminal telephone number 82 is a telephone number of a PHS contained in the portable terminal, such that the security controller 10 uses this telephone number to call up a lost portable terminal. The registrant ID 83 is the ID of the owner of the portable terminal, and the security controller specifies the user and security management data using this ID when performing a portable terminal information protection service. The verification information 84 is secret information (password) for confirming whether or not the one requesting a portable terminal information protection service is actually the registrant. The processing number 85 indicates the state of terminal information protection. The form (type) of terminal information protection is coded, for example, by setting "processing number = 1" if the information held by the terminal (protected information) is to be deleted, or setting "processing number = 2" if the information held by the terminal is to be deleted after the protected information has been recovered (transferred) to the security controller side, the form of information protection being pre-registered by the owner of the terminal. The encryption key B:86 is a public encryption key of a public key encryption format, used for encrypting information sent from the security controller to the portable terminal.

As shown in the data format 78, the data content 74 of the registration OK response 56 includes a registrant ID 83 and the processing number 85. The processing number 85 is designated by the user in the registration information message 53, and indicates a processing number accepted at the security controller side.

Fig. 4 illustrates an example of a data input screen displayed on a portable terminal for the registration procedures. 90 denotes a registration start screen, 91 denotes a registration information input screen and 92 denotes an owner confirmation screen, wherein the terminal owner inputs data sequentially in accordance with the displayed content. In the registration start screen 90, when "security registration" is selected from the menu 93, a registration window 94 is displayed. The registration window 94 has an emergency contact number used when requesting information protection when the terminal is lost, and "YES" and "NO" buttons for indicating whether information registration procedures are to be executed. The owner of a terminal which is to run an information registration process records this emergency contact number in a memo, and selects the "YES" button. Due to this operation, the portable terminal automatically dials the security controller 10, and when a connection is established, a registration request 51 is sent from the portable terminal to the security controller 10. The telephone number which is automatically dialed above is different from the above-described emergency contact telephone number. Additionally, the emergency contact telephone number can be made to be verifiable in the manual for the information protecting software loaded in the portable terminal.

The registration information input screen 91 has a registration information input window 95 formed based on the necessary data template 79 sent from the security controller 10 in the registration information

request message 52, where the terminal owner inputs data in a plurality of categories necessary as registration information (security management data records). When the input to all of the data categories has been completed and the owner selects the send button, a registration information message 53 having the content of the data format 77 as the data content 74 is generated, and sent to the security controller 10. The user confirmation screen 92 is a screen displayed by the portable terminal when a registration OK response 56 has been received from the security controller 10, displaying a user confirmation window 96 including an end button and registration information. When the owner selects the end button, the registration process is completed. At this time, a portion of the security management data, such as the registrant ID and password are stored in a non-volatile memory inside the portable terminal.

Fig. 5 shows an example of a flow chart for a processing program run by the security controller 10 during registration processing. Blocks 61, 62 and 63 correspond respectively to the registration acceptance operation 61, the registration information acceptance operation 62 and the registration information confirmation operation 63 shown in Fig. 2. the security controller 10 is in a state of awaiting incoming calls from the portable terminal (step 101), and repeats the standby state by means of a continual process (102) as long as there are no incoming calls. If a message is received, the message data (input data) is checked (103), and it is determined whether or not the received message is a registration request 51 (104). If a registration request 51, a registration information request data 52 is prepared, and after transmitting this to the portable terminal (106), the reception of the next message if awaited (107). If the above-described first message is not a registration request 51, another process 105 is performed.

When the registration information 53 which is encrypted with the encryption key A is received as the next message, the secret encryption key corresponding to the above encryption key A is applied to decode and analyze (108) the registration information, after which the registration information confirmation request message 54 is prepared and sent to the portable terminal (109), after which the next message is awaited (110). The data content 74 of the above-described registration information confirmation request message 54 contains the data content 77 of the registration information message 53 received by the security controller 10. When the registration confirmation response 55 is received from the portable terminal, the registration information which has already been received is registered as security management data (113), and a registration OK response is prepared and sent to the portable terminal (114). It is also possible to send a message having the same data content as the registration information message as a registration confirmation response 55 from the portable terminal side, and as indicated by the dashed line, to decode and analyze the data content of the received registration confirmation message 55, then comparing with the already received registration information (112), and performing the registration process (113) in the event of a match (113) and rerunning the process form the registration information request step (106) in the even of a non-match.

Fig. 6 shows the operational procedure of a protection system in the case where the owner of a lost portable terminal dials the emergency contact telephone number by means of, for example, push-button dialing (telephone), and requests information protection of the security controller 10. Here, an operational example shall be explained wherein at the time the request for information protection is received, the lost portable terminal is in a state of communicability with the PHS system, and the security controller 10 succeeds in accessing the lost portable terminal. Additionally, an operational flow chart for the security controller 10 which runs the operations S1:134-S5:138 in Fig. 6 and the operations S6:158-S7:159 in Fig. 7 to be described below are shown in Fig. 10, and the operations shall be described hereafter with reference also to the operational steps of Fig. 10.

When the owner who has realized that the portable terminal has been lost dials the telephone number of the emergency contact with the telephone 18 (operation U1:131), a connection is established with the security controller 10. In this case, the call control signal issued from the telephone when the call is made is a protection request 121. On the security controller 10 side, the incoming call to the above-described emergency telephone number is connected to the audio response system, and as the first automatic response message (verification confirmation message) 122, an audio message with the content,

for example, of "Please enter registrant ID and #, followed by password and #" is outputted (operation S1:134, steps 101-205 of Fig. 10). The owner uses the numerical keys and # button in reply to the above audio message to enter the registrant ID and password (operation U2:132). The inputted data is sent as verification data 123.

The security controller 10, upon receiving this verification data 123, retrieves the registered security management data record having the same ID as the registrant ID and determines whether the received password matches with the registered verification information 84, and after confirming that the requester of information protection is someone who is registered, outputs the requested confirmation message 124 (operation S2:135, steps 206-208 of Fig. 10). The above request confirmation message 124 may, for example, consist of: "Now commencing information protection operation. If the portable terminal is not found, the search operation shall be continued. If not found immediately, you will be contacted at a later date. Please press the telephone number to be contacted followed by the # button. Please wait."

If the owner inputs the telephone number and presses the # button (operation U3:133), the security controller indicates a PHS telephone number registered in the security data record for the PHS system DB 11, and sends a portable terminal search request 127 (operation S3:136, steps 209-211 of Fig. 10). The PHS system DB 11, upon received the above search request (127), searches the database to find whether a portable terminal having the relevant PHS telephone number has its position registered, and sends the result to the security controller 10 as a portable terminal search response 128 (operation N1:139).

If the target portable terminal has been position-registered, the security controller 10 indicates for the portable terminal the type of information protection with a pre-registered processing number 85, and sends an information protection instruction 129 (operation S4:137, steps 212-214 of Fig. 10). The portable terminal 14 which has received the information protection instruction 129 runs the information protection program, and upon completion, sends a protection completion report 130 along with protected data as needed to the security controller 10 (operation P1:140).

Upon receiving this protection completion report 130, the security controller 10, immediately if there is no protected data to be transferred, and after storing this in correlation with the security management data record if there is data to be transferred (transferred data record), responds to the information protection completion notification 126 (operation S5:138, steps 215-208 of Fig. 10) to end the procedure. The above-mentioned information protection completion notification 126 is an audio message consisting, for example, of "the protection of portable terminal information is complete", with an audio message to the effect that protected data has been recovered in the case where it has.

In the above embodiment, the portable terminal search request operation S3 with respect to the PHS system DB and the reply operation N1 thereto are effective when the PHS system DB, in response to the portable terminal search request 127, finds the base station in which the target portable terminal is position-registered, retrieves the bases station location (address) corresponding to the identifier of the base station, and for example, indicates the rough current position of the target portable terminal as a cell radius centered on the above base station location, and notifies the security controller thereof by means of the above portable terminal search response 128, upon which the security controller notifies the search requester of the above current position information. Additionally, as shown in Fig. 8,if the portable terminal is not in a state of communicability when the owner of the portable terminal requests information protection, it becomes effective when the position registration of this terminal in the radio network is detected and an information protection instruction is automatically issued.

If this type of terminal position information service for terminal owners is absolutely unnecessary, it is possible to omit the terminal search request 127 to the PHS system DB, and for the security controller 10 to attempt to setup a call (connection) to the target terminal with the above operation S3 regardless of whether or not the target portable terminal is position-registered, and to run operation S4 when a connection is established. If the target terminal is in a non-communicable state, the security controller 10 can be made to automatically repeat the calls in a predetermined repetition pattern.

Fig. 7 shows an operational example for the case where the lost portable terminal cannot be found at the time the request for information protection is received as shown in Fig. 6. IN the operational sequence of Fig. 7, the procedure until the PHS system DB 11 sends the security controller 10 a portable terminal search response 128 is the same as in Fig. 6. In this case, when failing to confirm the current position of the portable terminal for which there has been a search request from the security controller 10, it is useful to put up a flag indicating that this is a terminal which is being sought by the security controller 10 in the information record of the portable terminal at the PHS system DB 11 side. In this example, the security controller 10 receives a portable terminal search response 128 from the PHS system DB 11 indicating that the position confirmation has failed, and in operation S4:137, sends the owner an audio message (continual confirmation message) 151 consisting, for example, of "The portable terminal has not been found. The terminal will continue to be monitored. If you wish to discontinue the terminal search and information protection now, please press 2#. If you wish to continue, please press 1#." (step 219 in Fig. 10).

If the owner selects "2#", the security controller 10 outputs the audio message "The service is completed." (operation S6:158, steps 220, 221, 227 of Fig. 10) and the communications are terminated. If the owner selects "1#", in the above-described operation S6:158, an audio message (contact confirmation message) 153 consisting, for example, of "Please confirm that your contact telephone number is XXXXXXXXX. If correct, please press 1#. If you wish to change the telephone number, please press 2#, then the telephone number, and #" (step 221, 222 of Fig. 10). When the owner performs the response operation with respect to the confirmation message (operation U6:157), the security controller analyzes the content of the contact response 154 due to the above response operation, and if "1#", sends a termination message 155 consisting of "The service is completed.", and the communication is terminated. If "2#" and the telephone number are inputted in response to the above confirmation message, the telephone number confirmation message is resent, and the same operations are repeated (operation S7:159, steps 223-227 in Fig. 10).

Fig. 8 shows the operational procedure for a continual protection process for automatically finding lost portable terminals. Additionally, Fig. 11 shows an operational flow chart of a security controller 10 corresponding to the operations S8:166 and S9:167 of Fig. 8, which operation shall be described with reference to Fig. 11. When the lost portable terminal 14 is turned ON, the internal PHS telephone function issues a position registration request 161 to a base station, and the PHS system DB 11 performs a terminal position registration (operation 168). When the PHS system DB 11 receives the position registration information 161 from any base station, it finds the flag indicating that the terminal is being sought by the security controller 10 in the information record of the portable terminal during the position registration operation, and sends the security controller 10 a position registration notification 162 indicating the lost terminal position.

The security controller 10 is in a state of awaiting a position registration notification from the PHS system DB (step 101 of Fig. 11), and upon receiving the position registration notification 162, begins communicating with the lost portable terminal 14 by means of the PHS telephone system, sending the information protection instruction 129 (operation S8:166, steps 243-245 of Fig. 11). The portable terminal 14 responds to this information protection instruction 129, runs an information protection program such as shown in Fig. 6, and sends the security controller 10 a protection terminal report 130. Upon receiving this protection terminal report 130, the security controller 10, as indicated by the operation S9:167, stores any protection data that exists (records transfer data (steps 246-248 of Fig. 11)), and after recording the information protection termination in the security management data record, automatically dials the contact number of the terminal owner stored in the above data record, and gives an information protection report 165 with an audio message (steps 249-251 of Fig. 11). IN the above embodiment, the PHS system DB 14 checks for the presence of an information protection request and automatically notifies the security controller, but in the case where it is not desirable to add such a special function to the PHS system DB 14, it is possible for the security controller 10 to obtain a cue for the operation 8:166 by periodically calling the portable terminal.

Fig. 9 shows an example of the format of a message 70 transmitted between the portable terminal, security controller and PHS system database when running the above information protection operation. The basic structure of the message format 70 is similar to that shown in Fig. 3, with the data content 74 differing according to the type of message. 301 denotes the data content of the portable terminal search request message 127 shown in Figs. 6 and 7. It consists of the two fields of a processing instruction message 305 and a portable terminal telephone number 79, with a character string indicating the content of the request to the PHS system DB 11 being set in the processing instruction message 305, and the PHS telephone number of the portable terminal to be found being set in the portable terminal telephone number 79.

302 denotes the portable terminal search response 128 shown in Figs. 6 and 7, and the data content 74 of the message used in the position registration notification 162 shown in Fig. 8. The data content is composed of the three fields of the presence/absence of the portable terminal 310, the portable terminal telephone number 82 and the position information 306, with the PHS telephone number of the portable terminal which is to be found being set in the portable terminal telephone number 82, position information indicating the connection point (base station) inside the PHS system where the portable terminal is located being set as the position information 306, this position information enabling the rough current position of the portable terminal to be known.

303 denotes the data content 74 of the message of the information protection instruction 129 shown in Figs. 6 and 8, including a portable terminal identifier ID 81, a portable terminal telephone number 82, a registrant ID 83, verification information 84, a processing instruction 311 and an encryption key C:307. The portable terminal identifier ID 81, portable terminal telephone number 82, registrant ID 83, verification information 84 and processing number 85 are registered as security management data, and when the information protection instruction 129 is received, used for checking the reliability of the received message at the portable terminal 14 side. The encryption key C307 is a public encryption key according to the public key encryption format, the portable terminal using this encryption key C to encrypt the protection information sent to the security controller.

304 denotes the data content 74 of the message of the protection completion report 130 shown in Figs. 6 and 8, consisting of the two fields of a message type ID 308 and data 309. The message type ID 308 is set, for example, to "0" when the following data field 309 contains only a protection termination report code, "1" when it contains a protection termination report code and protected data and there is no more data, and "2" when there is data following the protected data. The content of the data field 309 is encrypted using the encryption key C307.

Fig. 12 is an operational flow chart of a PHS system DB running the operations N1:139 and N2:168 in Figs. 6, 7 and 8. The PHS system DB 11 checks the received messages (step 261), and if a received message is a position registration request, runs the operation N2:168. In this case, a normal position registration operation is performed (step 271), and if this portable terminal is found to be such as to have a search request issued by the security controller, prepares notification information for the security controller (position notification 162 of Fig. 8) (272), and after sending this to the security controller (273), returns to a message reception standby state.

When a portable terminal search request 127 is received from the security controller, the operation N1:139 is performed. In this case, the portable terminal search request is first analyzed (264), and the database information is searched based on the portable terminal telephone number designated by the search request (portable telephone number 79 indicated in Fig. 9) (265), and a check is made as to whether or not the target terminal has its position registered (266). If the target terminal has its position registered, a "1" indicating the existence of the portable terminal is placed in the field 310 of the data content format 302 shown in Fig. 9, the telephone number of the target portable terminal is placed in the field 82, and a response message 128 in which the base station information accommodating the above target portable terminal is prepared in the field 306 (267), and the result is sent to the security controller

(270). If the position of the target portable terminal is not registered, a response message 128 with a "0" set in the above fields 310 and 306 is prepared (268), and this is sent to the security controller (270).

Fig. 13 is a flow chart showing the details of the data protection operation P in the portable terminal to which the present invention is applied. When interrupted by the communication control portion while in a normal data processing operation state 282 (281), the portable terminal starts up special software for data protection stored in the ROM in the portable terminal, and analyzes the transmitted message (284). When the PHS telephone function and communication control portion are in a reception standby state and the power of the CPU main body portion is not turned on, the above-described communication message analysis is performed after automatically turning the CPU power on.

If the message received at the communication control portion which caused the interruption is an information protection instruction 129 from the security controller, then the data portion is encrypted by the encryption key B:86 as described in Fig. 3, so that in this case, the content of the message is decoded using a secret key pre-stored in the ROM corresponding to the encryption key B:86. If the above-described communication content is not an information protection instruction 129 (284), then the normal communication procedure (282) is performed, and if an information protection instruction, a verification check is performed (286). The verification check is performed by comparing the verification information contained in the information protection instruction (content of the field 85 in Fig. 9) and the proper owner verification information stored inside the portable terminal when registering for portable terminal information protection (password). If there is a problem as a result of the verification, then the subsequent procedures are skipped and the procedure is returned to step 281.

If there is no problem in verification, then the content of the protection instruction is analyzed (287), the necessity of data transfer is determined from the value in the processing number field 85 (288), and the procedure advances to step 291 if there is no need for data transfer. If data transfer is required, then the encryption key in the information protection instruction (encryption key C:307) is used to encrypt the terminal information (protected data) (289), and after the encrypted terminal information is sent to the security controller (290), the procedure advances to step 291. In step 291, a terminal information privacy protection (invalidation or overwrite) procedure is performed (291). The data privacy protection can be achieved, for example, by deleting the terminal information from memory or by converting it to false data. When the data privacy protection is completed, a data protection completion message is sent to the security controller (292), the interruption is terminated and the original state is resumed.

Fig. 14 shows the structure of a security controller 10. The security controller 10 comprises a CPU 20, a ROM 21, a RAM 22, a data file 23, a communication control portion 24, a communication interface with the PHS system DB 25, a communication interface 26 with the portable terminal, an audio control portion 27 having an audio reply function, a telephone interface 28 and an internal bus 29. The CPU 20 controls the communication control portion 24 and audio control portion 27 according to a control program prepared in the ROM 21, and communicates with the PHS system DB through a communication interface 25, with portable information terminals through a communication interface 26 and with telephones through a telephone interface 28. The RAM 22 is used as a work area for a program, and is used for temporary storage of data from a PHS system DB or portable terminal owner. The file device 23 is used to store security management data records, data removed from lost terminals, or information necessary for stationary protection processes.

Fig. 15 is a block diagram showing the structure of a portable terminal 14. The portable terminal 14 to which the present invention is applied comprises a CPU 31, a ROM 32, RAMs 33A and 33B, an auxiliary memory device 34, a display device (e.g. a liquid crystal display) 35, an input device 36, a power supply control portion 37, a communication interface 38, a communication control portion 39, a bus 40, a power supply control line 41 and a communication interruption control line 42. The CPU 31 passes data between the ROM 32, RAMs 33A and 33B, the auxiliary memory device 34, the display device 35, the input device 36, and the communication interface 38 through the bus 40. Additionally, the power supply control portion 37 controls the power supplies of the various elements described above so as to turn them

on or off through the power supply control line 41. In the present invention, the communication control portion 39 has functions for achieving PHS radio communications, such as for example, an antenna, a high frequency circuit, and PHS communication procedure control and communication content check means, such as to exchange communicated message data with the CPU 31 through the communication interface 38 for normal PHS communications, generate a communication interruption control signal to interrupt the CPU 31 or power supply control portion 37.

The ROM 32 contains various types of software for achieving the functions of a portable terminal, and special software and control information for achieving terminal information protection according to the present invention. The RAMs 33A and 33B are backed up by a power supply, with the RAM 33A being for storage of normal data which does not require information protection, and the RAM 33B being used for storage of specific file data to be protected by applying the present invention. When interrupted by the communication control portion, the CPU of the portable terminal runs special software provided in the ROM 32, and if the interruption is due to reception of a terminal information protection instruction, runs the above-mentioned data recovery and protection procedures with the information stored in the RAM 33B as the object.

In the above embodiment, the information to be protected in each terminal is stored in a special memory, and the information protection operation is performed with respect to all information in this special memory when the terminal is lost, but the information protection can also be performed simply by specifying a data file name. For example, it is possible to manage the information which is to be protected using a special file name or a filed name with a specific abbreviation in each portable terminal, and to have the terminal owner specify a file name (or file discrimination information such as abbreviations) to be protected when requesting registration for information protection, store this in the above-described special software, and run the protection process on files with these special file names when an information protection instruction is issued.

Additionally, in the embodiment, a terminal owner directly interacts with the security controller through a telephone, and the security controller side controls acceptance of information protection according to an audio response function, but it is possible to have the owner of the lost terminal access the security controller from another radio terminal having a text data transmitting function or another terminal connected to the network 5, so as to exchange the information required for terminal information protection in a data message format. Additionally, the information protection can be performed by having an agent at the security system side receive an information protection request reported by a normal telephone by the owner of a lost terminal access the security controller from a special terminal, and input the data such as passwords necessary for verification of the owner through the agent terminal.

Effects of the Invention

As is clear from the above explanation, the present invention does not require troublesome operations such as password input in order to confirm file access rights when using the portable terminal normally, but enables the terminal information to be protected or the information to be recovered when the portable terminal is lost. Additionally, if the terminal position registration function in the radio network is used for requesting information protection, the approximate current position of the lost terminal can be known, thus aiding in finding the lost terminal due to this position information.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 A structural diagram of a network system for achieving portable terminal information protection according to the present invention.

Fig. 2 A diagram showing an embodiment of the registration procedure for terminal information

protection.

Fig. 3 A diagram showing an embodiment of a message format transmitted between the portable terminal and the security controller at the time of registration for terminal information protection.

Fig. 4 A diagram showing an embodiment of a screen displayed on the portable terminal at the time of registration for terminal information protection.

Fig. 5 A flow chart showing an embodiment of the procedures of the control program executed by the security controller at the time of registration for terminal information protection.

Fig. 6 A sequence diagram showing an example of an information protection procedure run by the network executed when a terminal is lost.

Fig. 7 A sequence diagram showing another example of an information protection procedure run by the network executed when a terminal is lost.

Fig. 8 A sequence diagram showing another example of an information protection procedure run by the network executed when a terminal is lost.

Fig. 9 A diagram showing an embodiment of a message format transmitted during information protection.

Fig. 10 A flow chart showing an embodiment of a control program run by the security controller during information protection.

Fig. 11 A flow chart showing another embodiment of a control program run by the security controller during information protection.

Fig. 12 A flow chart showing an embodiment of a control program run a PHS database system during information protection.

Fig. 13 A flow chart showing an embodiment of a control program run by a portable terminal during information protection.

Fig. 14 A block diagram showing an example of the structure of a security controller.

Fig. 15 A block diagram showing an example of the structure of a portable terminal.

Description of Reference Numbers

1	radio network system
5	wire network
10	security controller
11	PHS system database
12	base station
14	portable terminal
18	telephone
51	registration request
52	registered information request

53	registered information
54	registered information confirmation
55	registration confirmation reply
56	registration OK response
70	transmission message format
71	identification ID
72	action ID
73	data quantity
74	data content
75	CRC
76	registration request data
77	registered information data
78	registration OK response data
90	registration start screen
91	registration input screen
92	owner confirmation screen
121	protection request
122	verification confirmation message
123	verification data
124	request confirmation message
125	request transmission
126	end notification
127	portable terminal search request
128	portable terminal search response
129	information protection instruction
130	protection end report and protected data
151	stationary confirmation message
152	stationary response
153	contact address confirmation message
154	contract address response
155	end message
301	portable terminal search data
302	portable terminal search response data
303	information protection instruction data
304	protected data